



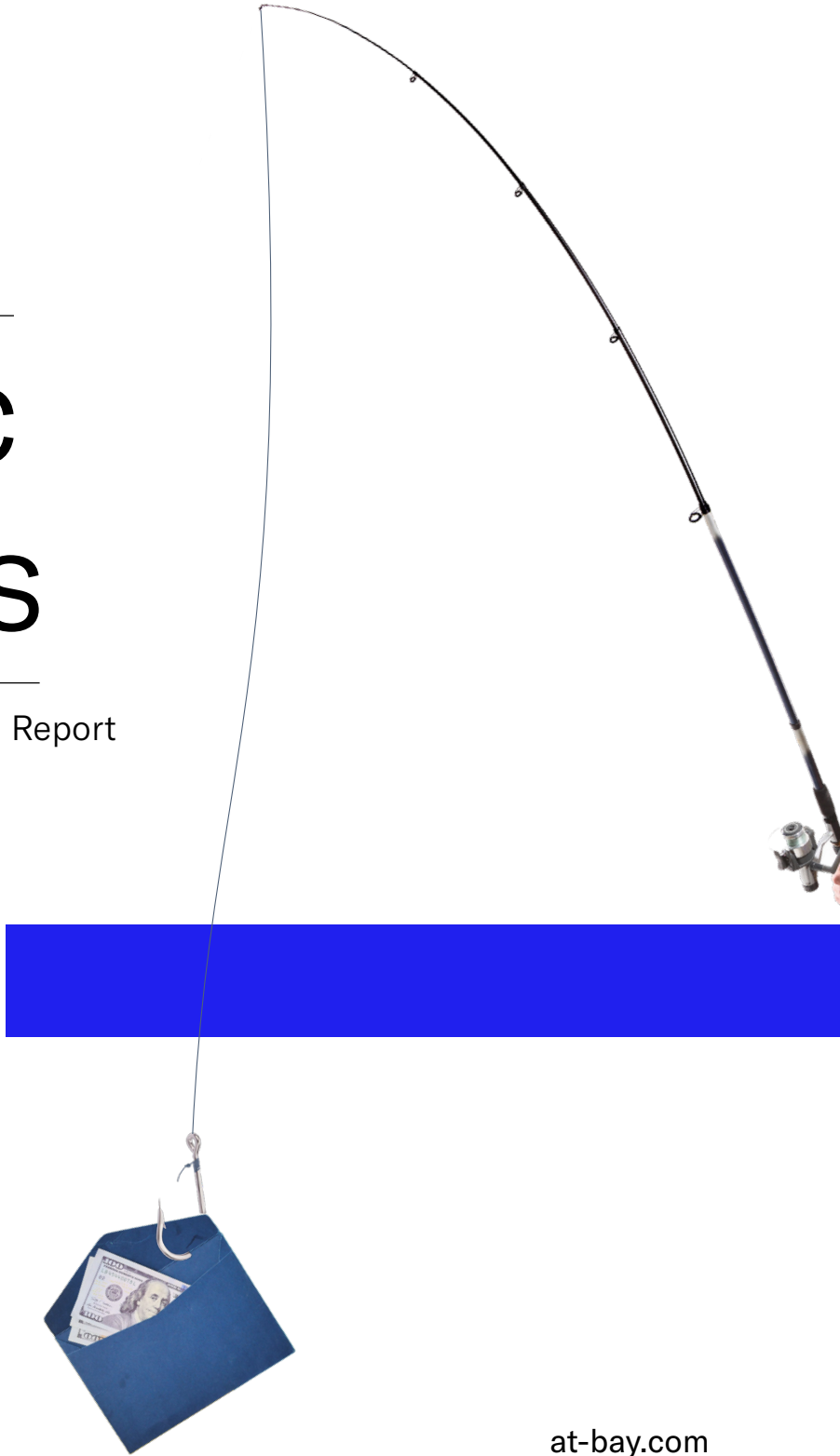
2024

---

# InsurSec Rankings

---

Email Security and Financial Fraud Report



# An analysis of At-Bay claims and cybercrime data



# Table of Contents

Introduction	4
Key Findings	5
Chapter 1: The Email Claims Landscape	6
Chapter 2: Email Security Solutions Rankings	9
Chapter 3: Email Solutions Rankings	13
Chapter 4: Anatomy of Financial Fraud	15
Conclusion	22
Methodology	24

# Introduction

Email is the most common cyberattack vector for businesses, serving as the most prevalent initial entry point to launch financial fraud, ransomware, and data breach attacks. Email plays an integral role in today's business operations, powering everything from basic communication, to sales, marketing, and finance systems. Cyberattackers do not overlook this opportunity, as email remains an under-secured asset that relies on easy-to-abuse technology, resulting in hundreds of billions of dollars lost every year<sup>1</sup>.

Email solutions and security gateways are a proactive measure that can improve overall security, but not all solutions yield the same outcomes. In this second annual report, we analyze over 55,000 policy-years of cyber claims data to understand which email solutions are most effective at reducing cyber risk stemming from email. We compare outcomes for the two most popular email solutions, Microsoft 365 and Google Workspace, and rank the best (and worst) email security solutions, based on real-world incidents experienced by At-Bay policyholders.

In 2023, the most common type of email attack (financial fraud), resulted in cybercriminals stealing an average of \$219K from unsuspecting businesses in At-Bay's portfolio. In the most severe cases, threat actors stole more than \$5M, leading to not only devastating financial impact for those businesses, but also operational and reputational fallout as well.

These financial fraud schemes are more complex than ever, varying from sophisticated social engineering techniques to compromising business email servers, but they all share a common theme: Nearly all financial fraud occurs via email. In 2023, 9 in 10 financial fraud claims for small and medium-sized businesses originated from email.

Our aim is to compile the most robust, data-driven assessment of email security solutions in an effort to reduce risk, improve outcomes, and create a more secure environment for businesses large and small. We are continuing this work because we believe in using data to improve security by equipping vendors with insights that drive product development and decision making, while empowering customers to make better choices in selecting secure software.

In 2023, **9 of 10** financial fraud claims for small and medium-sized businesses originated from email.

<sup>1</sup> Nasdaq and Oliver Wyman, 2024 Global Financial Crime Report, 2024; <https://www.nasdaq.com/global-financial-crime-report>

# Key Findings

1

## EMAIL CLAIMS FREQUENCY GREW 24% IN 2023

At-Bay's email claims frequency grew in 2022 and again in 2023, then dropped back to 2022 levels in the first half of 2024. This trend was consistent across all revenue bands, although the largest companies in our portfolio (those with \$100M+ in revenue) saw the lowest level of decline in 2024 and maintained the highest overall frequency.

2

## BUSINESSES USING MIMICAST FOR EMAIL SECURITY EXPERIENCED 37% FEWER INCIDENTS THAN THE AVERAGE

Only two email security solutions were correlated with better outcomes than the average: Mimecast and Proofpoint. For the second year in a row, businesses in At-Bay's portfolio that used Mimecast saw the lowest email claims frequency, and experienced an impressive 37% fewer incidents than the average.

3

## COMMON MX RECORD MISCONFIGURATIONS ARE PRESENT IN 7% OF CLAIMS

7% of claims have misconfigured MX records, which renders email security solutions ineffective. These misconfigurations are both easy for threat actors to discover and easy to exploit, opening the door to potentially damaging cyberattacks.

4

## COMPANIES USING GOOGLE WORKSPACE EXPERIENCED 3X LOWER CLAIMS FREQUENCY THAN THAT OF COMPANIES USING MICROSOFT 365.

Organizations in At-Bay's portfolio that used Google Workspace experienced the lowest frequency of incidents on average. Compared to the average for all email providers analyzed, Google's claims frequency was 54% lower — an improvement from the last report, which found businesses that used Google saw 41% lower claims frequency.

5

## FINANCIAL FRAUD ACCOUNTED FOR 61% OF EMAIL-RELATED CLAIMS IN 2023

Financial fraud was the most common cybercrime committed via email, accounting for 61% of At-Bay email claims in 2023. In the first half of 2024, that number jumped to 72%. 9 of 10 financial fraud claims originated from email.

6

## THE AVERAGE AMOUNT OF FUNDS STOLEN IN A FINANCIAL FRAUD INCIDENT WAS \$219K

In the most severe cases, threat actors stole more than \$5M. The real estate industry saw the worst financial fraud cases with an average stolen funds amount of \$434K.

7

## BUSINESS EMAIL COMPROMISE ACCOUNTED FOR 63% OF ALL FINANCIAL FRAUD CLAIMS

Financial fraud is becoming more sophisticated. Attackers don't just rely on social engineering for their efforts. They also increasingly use compromised email servers to achieve their goals. In half of all financial fraud BEC incidents, the At-Bay policyholder was compromised. In the other half, it was the vendor or partner who was compromised.

For this report, we define an "email claim" as a claim where email was the initial attack vector. This may include a malicious email that contains phishing links or malware, as well as attacks that were simply enabled by an email, such as a message that elicited a malicious action, but wasn't itself overtly malicious.

CHAPTER 1

# The Email Claims Landscape

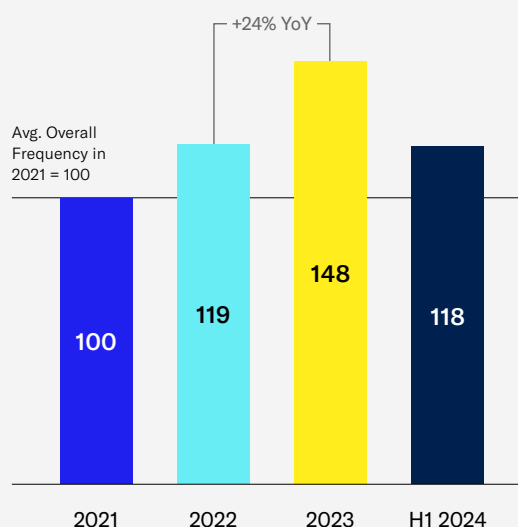
## Email Claims Frequency Grew 24% in 2023

Incidents where email is the initial attack vector are among the most prevalent attacks on businesses and continue to see elevated levels since 2021. Email claim frequency rose 19% from 2021 to 2022, and jumped another 24% in 2023. Despite a 20% decline in the first half of 2024, email frequency during this time period remained nearly equal to 2022 and 18% above 2021 levels.

It's possible this slight reduction in frequency could also be attributed to At-Bay's underwriting selection process and efforts to improve the quality of security and reduce risk in our portfolio, however email-related incidents remain present and financially perilous for businesses.

## Email Claims Frequency Increased in 2022 and 2023, Dipped in H12024

Figure 1: Indexed Email Claims Frequency by Year



Email-related incidents remain present and financially perilous for businesses.

## Email Claims Frequency by Company Annual Revenue

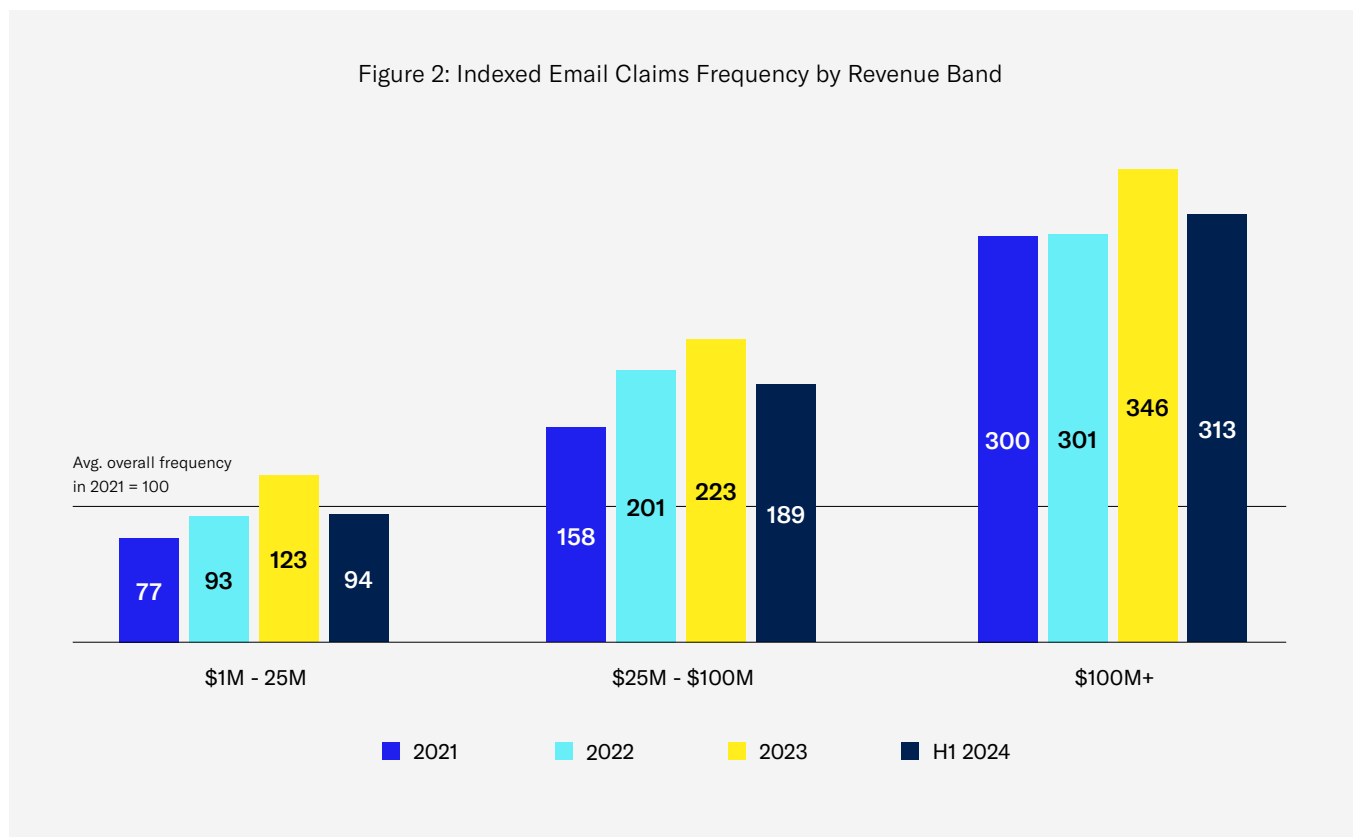
In 2022 and 2023, companies of all sizes saw steady increases in email claims frequency. Those with revenue greater than \$100M were more frequently the victim of email incidents in each period analyzed. In the first half of 2024, those companies had a 3X higher claim frequency than companies with annual revenue below \$25M. While all company sizes saw a dip in email claims frequency in the first half of 2024, businesses with \$100M+ in revenue only saw a slight decrease, remaining above 2021 and 2022 levels.

These findings are consistent with our previous research. Larger companies — who are more attractive targets for bad actors — are typically attacked more frequently than small ones, across

all types of attacks. Larger companies tend to have larger financial transactions, payments, and bank balances, which make for more enticing targets. They also have more vendors and partners, which leads to more payments and communications to potentially intercept.

Large operations mean potentially multiple layers of management which can create uncertainty around who makes decisions or authorizes payments, in addition to generally larger numbers of employees with email access, giving attackers more entry points for social engineering to succeed.

### Companies over \$100M in revenue experienced 3X more email claims than companies under \$25M



## Email Claims Frequency by Industry

Although we've seen a consistent trend in email frequencies over the years across revenue bands, the same cannot be said when viewed through the lens of various industry segments.

Companies in the manufacturing industry had the highest email claims frequency in the first half of 2024 and it was among the top industries for claims in the previous three years. Manufacturing is a prime target for cyberthreats as these companies are often receiving large volumes of raw materials and shipping lots of goods, typically with high value transactions and invoices that may be intercepted via an email attack. In addition, manufacturing businesses tend to have older, legacy systems, and poorer security overall.

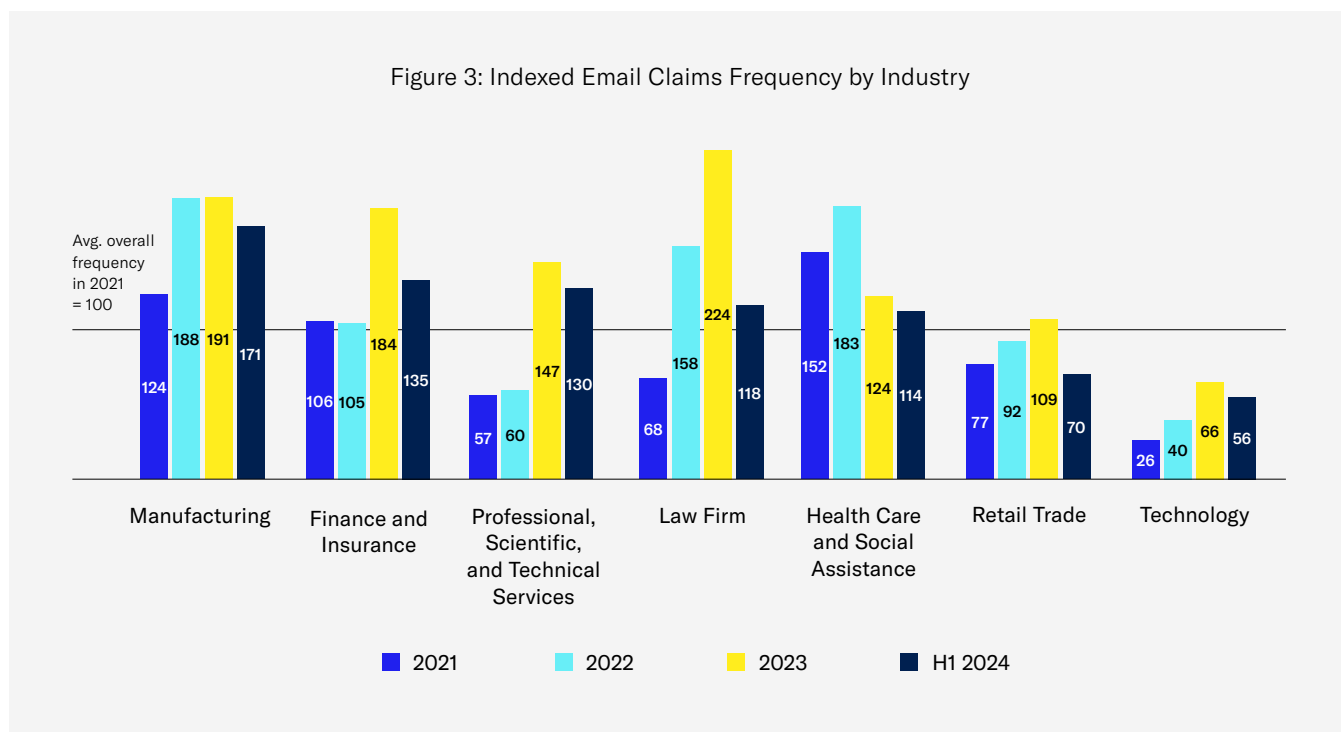
Finance is another industry commonly associated with high email claims frequencies. This is likely due to the comparatively higher volume of financial

transactions and wire transfers at these firms, making them potentially lucrative targets for threat actors to intercept.

Law firms saw particularly high email claims frequency in 2023, leading all industries in email claims frequency, before dropping 47% in the first half of 2024. This steep decrease is likely a direct result of At-Bay's deliberate action to improve the security controls of law firms in our portfolio after seeing a spike in 2023.

The technology sector performed relatively well in this regard, consistently seeing the lowest email claims frequency, well below the average. In the first half of 2024, technology companies were 3X less likely to be hit with an email attack than manufacturing companies.

### Manufacturing Sees the Highest Claim Frequency, Technology the Lowest





## CHAPTER 2

# Email Security Solutions Rankings

## A Comparison of Outcomes by Email Security Solution

While implementing an email security solution may be a proactive step in safeguarding your business, the presence of an email security solution does not guarantee comprehensive protection against cyberattacks. Evolving threats and the varying quality of solutions play a significant role in outcomes.

In addition, businesses continue to encounter a multitude of security challenges that stem from the complexity of implementing and managing such solutions. In our research, we found significant rates of misconfigurations that can lead to serious vulnerability and risk. In addition to the solution itself, how it is implemented matters, as does how easy it is to implement.

In this section, we analyzed claims and cyber crime data to compare outcomes for email security solutions when under the real-world stress of opportunistic threat actors. To do this, we analyzed email-related claims where an email security solution was in place to calculate the normalized claims frequency.

This is not a technical analysis of the functionality of the email solution, although after two years we have seen clear patterns in the outcomes of customers using certain solutions leading us to believe some are more effective than others at mitigating the risk of incidents involving emails.

The table below is a representation of those calculations, and shows the relative effectiveness of email security solutions in mitigating the risk of security incidents compared to the average — and each other. We have included every email security solution that was present in our previous report for completeness, although it's important to note Intermedia and Sophos have a small sample size in this year's analysis due to comparatively low market share.

Businesses using Mimecast for email security experienced **37%** fewer incidents than the average.

## Mimecast Customers Saw the Best Outcomes for the Second Year in a Row

Figure 4: Email Security Solution Rankings by Claims Frequency

Email Security Solution	Email Claims Frequency	Email Risk Index
Mimecast	0.073%	63 ▲ -15
Proofpoint	0.104%	89 ▲ -17
Intermedia <sup>*</sup>	0.118%	102 ▼ +13
Barracuda	0.148%	128 ▼ +10
Appraver	0.155%	134 ▼ +40
Sophos <sup>*</sup>	0.189%	164 ▼ +79
<b>Average Frequency of ALL At-Bay Customers with Email Security Solution</b>	<b>0.116%</b>	<b>100</b>

\*Small sample size due to market share

▲ Email Risk Index Improved vs. 2023 Report

▼ Email Risk Index Got Worse vs. 2023 Report

### Analysis

In most cases, customers with the listed security solutions do not see a reduction in risk for email-related incidents relative to the average. Customers of only two email security solutions (Mimecast and Proofpoint) experienced better than average outcomes.

For the second year in a row, businesses using Mimecast saw the lowest email claims frequency, experiencing an impressive 37% fewer incidents than average. These businesses saw 1.6X better outcomes than the average and 1.4X better than the next closest solution, Proofpoint.

Proofpoint customers experienced 11% lower frequency versus the average, 1.1X better outcomes than the average and an overall improvement in email risk index score from last year.

Only businesses using Mimecast and Proofpoint saw better outcomes this year when compared to last year. Customers using all other email security solutions saw less favorable outcomes since our last report.

Both Barracuda and Appraver clients saw worse outcomes compared with the previous report. Barracuda customers experienced a nominal increase in Email Risk Index Score by 10 points, while Appraver customers saw a significant increase in email claim frequency, jumping 40 points. Businesses using Sophos saw the largest jump in email claim frequency compared to the previous report, moving 79 points on the Email Risk Index and dropping into the lowest spot on the rankings. Compared to Mimecast, Sophos customers see 2.6X worse outcomes. However, the small sample size due to low market share should be taken into consideration.

SPOTLIGHT

## Email Security Solution Misconfigurations

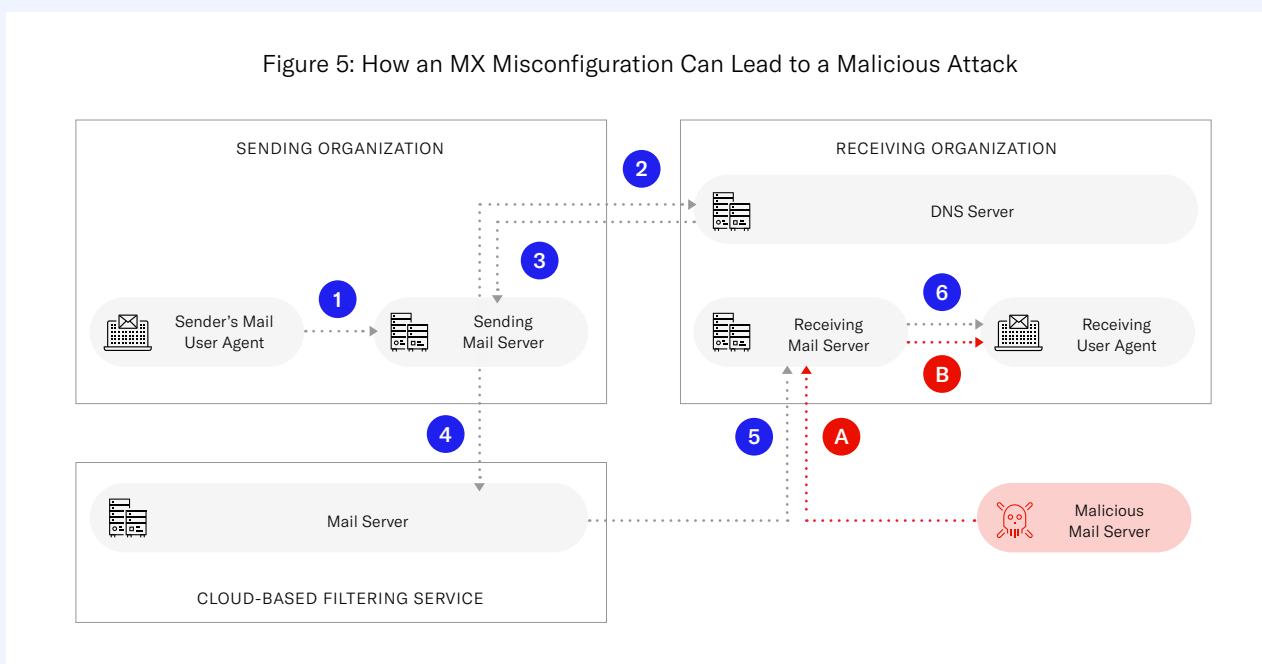
A DNS ‘mail exchange’ (MX) record directs email to a mail server, indicating how email messages should be routed. As shown in Figure 8, a properly configured MX record for a business using an Email Security Gateway will route all incoming emails (1) via a DNS server (2, 3) to the email security solution (4) before it passes to the receiving mail server (5) and onto the receiving user (6). A misconfigured MX record, however, allows email traffic to be sent directly to the email server (A), bypassing security solutions and delivering unfiltered mail to the receiving user (B), exposing businesses to potential security risks.

In our analysis, we found that 7% of claims have misconfigured MX records. MX record misconfiguration can happen for a host of reasons, including human error, lack of expertise or understanding of the configuration settings, software bugs or glitches, system updates or changes, or malicious actions by unauthorized individuals.

When these records are misconfigured, either intentionally or inadvertently, it allows attackers to bypass the security solution meant to keep an organization’s email safe, rendering it ineffective.

Attackers can exploit these misconfigurations to intercept, manipulate, or divert email communications, allowing them to launch targeted attacks or gain unauthorized access to confidential data.

Other research has similarly uncovered this issue. In a study by the University of California San Diego in 2024<sup>2</sup> that analyzed thousands of domains, researchers tested these vulnerabilities in an academic environment, finding the misconfigurations did leave a significant number of domains vulnerable to potentially harmful email.



<sup>2</sup> Samantha Rao, et. al., Unfiltered: Measuring Cloud-based Email Filtering Bypasses, 2024; <https://www.sysnet.ucsd.edu/~voelker/pubs/unfiltered-www24.pdf>

Some vendors are associated with a much higher rate of misconfigurations than others. For example, nearly 12% of customers with Barracuda and 11% of Proofpoint customers had an MX misconfiguration present. Customers of Mimecast and Appraver saw misconfiguration rates of 6.4% and 5.8% respectively, nearly half of the rates of Barracuda and Proofpoint customers.

This phenomenon is not yet being exploited at scale and we have not yet seen it as a driver of claims, but it has all the hallmarks of becoming a major entry vector for cyberthreats. Should these common misconfigurations be exploited at scale it will certainly drive loss. These misconfigurations are both easy for threat actors to discover and easy to exploit, opening the door to potentially damaging data breach, financial fraud, and ransomware attacks. There is inherent risk correlated with misconfiguration and it is something we believe email gateways and their customers should be aware of and prioritize.

### Over 11% of Companies with Barracuda and Proofpoint Have Misconfigured MX Records

Figure 6: Percentage of Organizations with Misconfigurations by Email Security Solution

Email Security Solution	Misconfiguration Rate Among All Policyholders
Barracuda	11.93%
Proofpoint	11.30%
Sophos	9.32%
Intermedia	7.58%
Mimecast	6.40%
Appraver	5.84%

This phenomenon is not yet being exploited at scale and we have not yet seen it as a driver of claims, but it has all the hallmarks of becoming a major entry vector for cyberthreats.

CHAPTER 3

# Email Solutions Rankings

## A Comparison of Outcomes by Email Solutions

Email solutions are the underlying technology that powers email. Some companies do not overlay it with an email security solution for whatever reason, be it choice, cost, or capability. We analyzed claims frequency for the businesses using the most common email solutions (Google Workspace, Microsoft 365, and Microsoft Exchange) to compare outcomes for each product.

Similar to our previous report, this analysis excludes organizations that have paired an email solution with an email security solution for a layered approach because we wanted to understand the outcomes related with each solution on its own.

The table below shows the individual email claims frequencies of the email solutions most used by our customers.

### Google Workspace Customers Saw the Best Outcomes for the Second Year in a Row

Figure 7: Email Solution Rankings by Claims Frequency

Email Solution	Email Claims Frequency	Email Risk Index
Google Workspace	0.053%	46 ▲ -13
Microsoft 365	0.168%	145 ▼ +27
Microsoft Exchange	0.180%	155 ▲ -4
<b>Avg. Frequency for ALL</b>	<b>0.116%</b>	<b>100</b>

▲ Email Risk Index Improved vs. 2023 Report

▼ Email Risk Index Got Worse vs. 2023 Report

## Analysis

Organizations that used Google Workspace experienced the lowest frequency of incidents on average. Compared to the overall average, Google's claims frequency was 54% lower — an improvement from the last report, which had found businesses using Google saw 41% lower claims frequency than average.

Businesses using Microsoft 365, by contrast, had a relative claims frequency 45% higher than the overall average, seeing worse overall outcomes compared to last year's report.

The gap in outcomes for businesses who use either Google or Microsoft 365 has grown in this year's report. Companies using Google Workspace experienced 3X lower claims frequency than that of companies using Microsoft 365.

Market share likely plays at least a partial role here. Microsoft 365 has a significantly larger market share compared to Google Workspace, making it a more attractive target for cybercriminals looking to maximize their impact<sup>3</sup>. Attackers often prioritize attacking platforms that are widely used, as this increases the likelihood of successful attacks and allows them to potentially reach a larger number of organizations more efficiently.

However, Google Workspace also includes by default many security features that may not be the default setting in other email solutions, such as real-time scanning for phishing emails and malicious attachments, automatic security updates to protect against vulnerabilities, and integrated threat intelligence to proactively identify and respond to potential threats. These default security features provide organizations using Google Workspace with a comprehensive and robust security framework out of the box, without requiring additional attention to set up or configure.

Businesses using on-premises Microsoft Exchange instances saw 55% more incidents than average. On-premises solutions are generally harder to manage and keep up to date, especially for small- and medium-sized businesses that often lack the expertise and resources to effectively manage their IT infrastructure. Combine this with the fact that many companies are running older, unsupported versions of Exchange, and it makes using an on-premises instance of Microsoft Exchange a comparatively much larger risk.

Considering these challenges, At-Bay strongly recommends transitioning to a cloud-based email solution to mitigate security risks and ensure proactive vulnerability management.

<sup>3</sup> IBM, X-Force Threat Intelligence Index 2024, 2024; <https://www.ibm.com/reports/threat-intelligence>

---

Companies using Google Workspace experienced **3X** lower claims frequency than that of companies using Microsoft 365.

## CHAPTER 4

# Anatomy of Financial Fraud

## Financial Fraud Accounted for 61% of Email Claims in 2023

Among all email-related claims, one type of incident stands out as the most prevalent year after year: financial fraud. Financial fraud refers to the criminal act of using technology to steal funds from individuals or organizations. This can include various fraudulent activities, such as identity theft, phishing scams, or sophisticated technical breaches that lead victims to unknowingly send funds to illicit recipients.

Financial fraud poses a significant threat to businesses, accounting for more than \$485 billion globally in 2023, according to a report by Nasdaq and Oliver Wyman<sup>4</sup>. While the monetary loss may be the most striking, victims of financial fraud may also suffer from legal repercussions, damage to reputation, and the erosion of customer trust and confidence.

In 2023, financial fraud accounted for 61% of all email claims, jumping 11 points in the first half of 2024 to 72%, its highest level in at least three years.

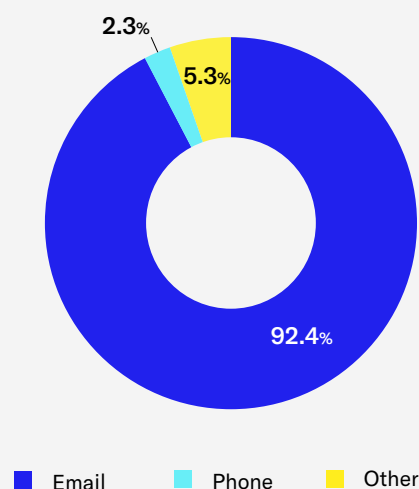
In addition, financial fraud is overwhelmingly an email-centric problem as 92% of financial fraud claims start with email, with only a small fraction using other channels, such as phone or text messaging.

<sup>4</sup> Nasdaq and Oliver Wyman, 2024 Global Financial Crime Report, 2024; <https://www.nasdaq.com/global-financial-crime-report>

While email security solutions may be capable of protecting businesses from technical attacks, it is the human element that makes preventing financial fraud so challenging. Stopping malicious or suspicious emails and protecting against technical attacks is just one layer of defense, but it won't prevent an employee from mistakenly sending a wire transfer to a fraudulent account because they did not follow the proper verification processes. However, a combination of email security, identity management and control, plus processes and training can lead to significantly lower risk.

## 92% of Financial Fraud Incidents Occur Via Email

Figure 8: % of Financial Fraud Incidents by Communication Channel



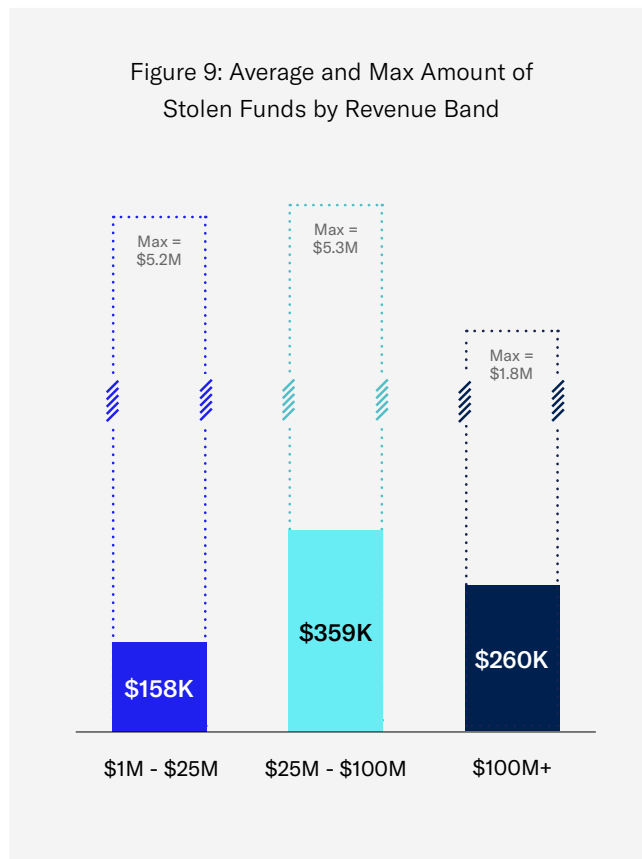
## The Average Financial Fraud Incident Cost \$219K

Financial fraud losses can be substantial. The average amount of funds stolen in a financial fraud incident is \$219K across all segments. In the most severe instances, businesses lost more than \$5M in a single fraud event. This makes for a devastating financial loss for any company.

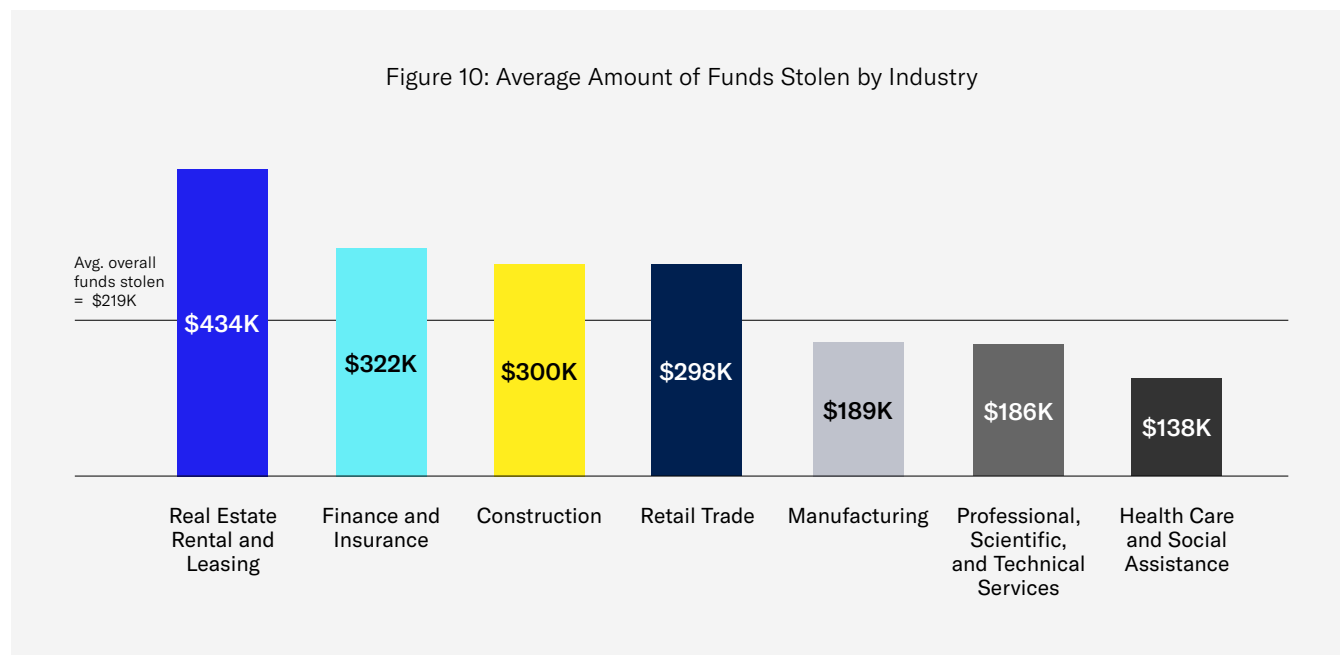
Real estate companies took the top spot for funds stolen at \$434K, nearly 2X the average. This is likely attributable to cybercriminals taking advantage of the frequent and high value wire transfers made during real estate purchases. It's likely a similar story for finance companies, an industry with a high volume of transactions being made and which saw average funds stolen amount of \$322K, almost 50% above the average.

Manufacturing and healthcare, despite being some of the most frequently targeted industries for email attacks, were below the average in terms of stolen funds from financial fraud.

## Companies Lost More Than \$5M in the Most Severe Cases of Financial Fraud



## Real Estate, Finance, Construction, and Retail See the Highest Average Funds Stolen Amounts

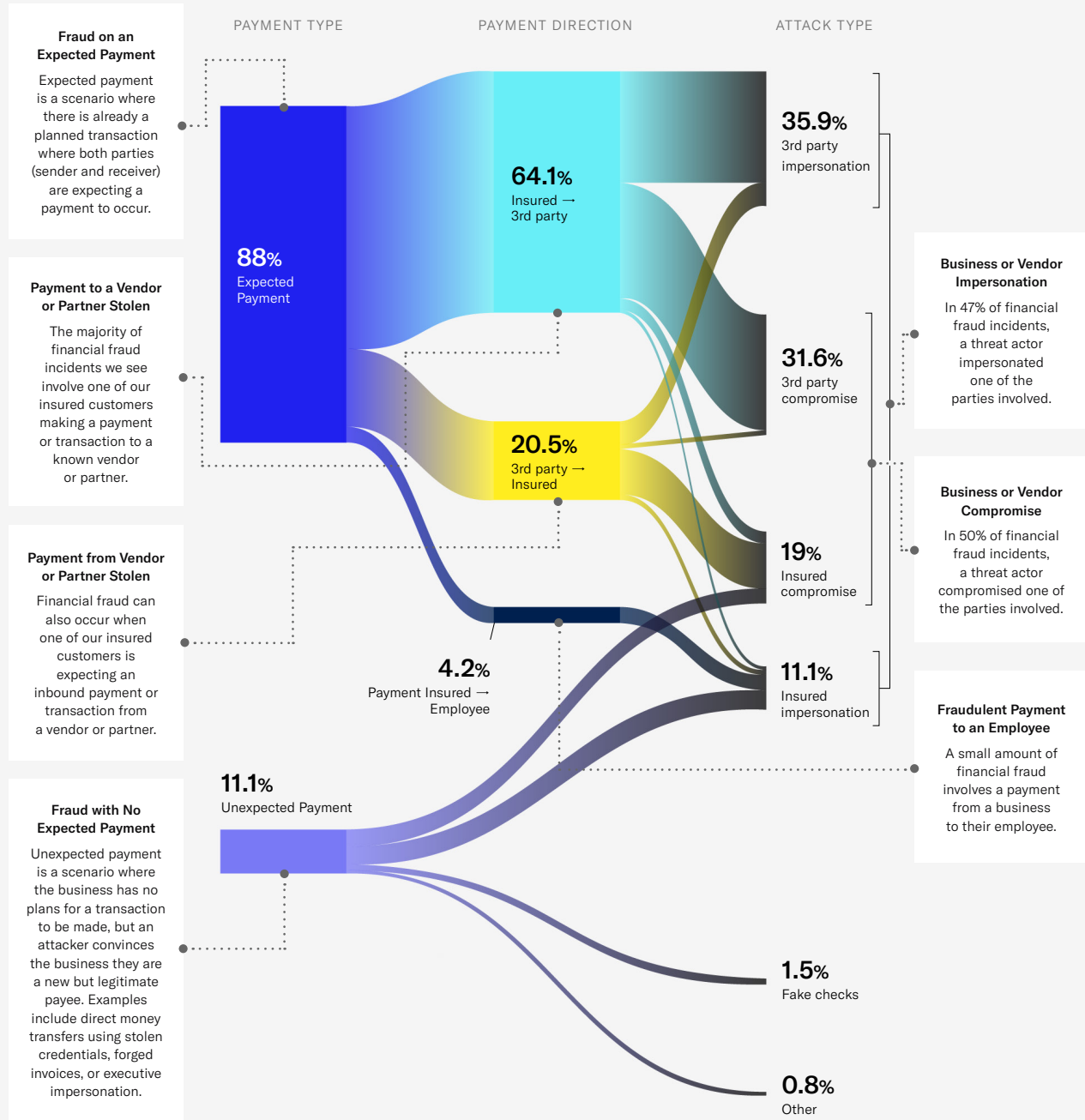




## The Anatomy of Modern Financial Fraud

Financial fraud can happen in a variety of ways using a variety of tactics, making it particularly challenging to detect and prevent. We broke down claims and cyber crime data to illustrate the various ways financial fraud can take shape.

Figure 11: Financial Fraud Visualized



Source: At-Bay Claims and Cybercrime Data, 2024 InsurSec Rankings Report

## How Financial Fraud Happens

The vast majority (88.9%) of financial fraud happens when there is an expected payment in progress. This means the attacker has somehow gained knowledge of a payment being made and has inserted themselves into the middle of that process, disrupting and redirecting a payment.

We see this primarily playing out in two ways:

In 64% of the cases, payment is due from one of our insured businesses to a third-party vendor, partner, or customer (Figure 13). About half of these instances involve a threat actor impersonating a third-party and tricking the victim into believing they are the vendor or partner to steal funds. The other half of these incidents involve a threat actor compromising a third-party vendor or partner, gaining access to the third-party's systems and redirecting funds using the third-party's legitimate email account.

In 20% of the cases, payment is due from a third-party vendor to one of our insured businesses (Figure 14). In most of these cases, the insured business was compromised, meaning a threat actor hacked into the insured business's systems, typically using their email to impersonate the insured and communicate with the vendor, convincing them to redirect payment.

## Common Financial Fraud Scenarios

Figure 12: Threat Actor Redirects Funds from a Business

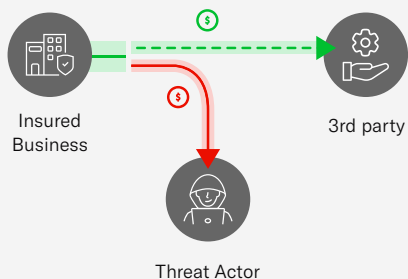
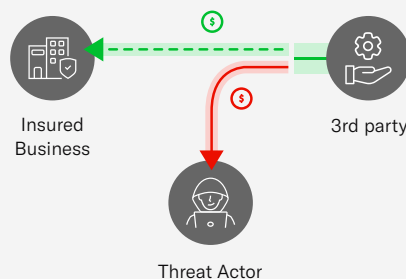
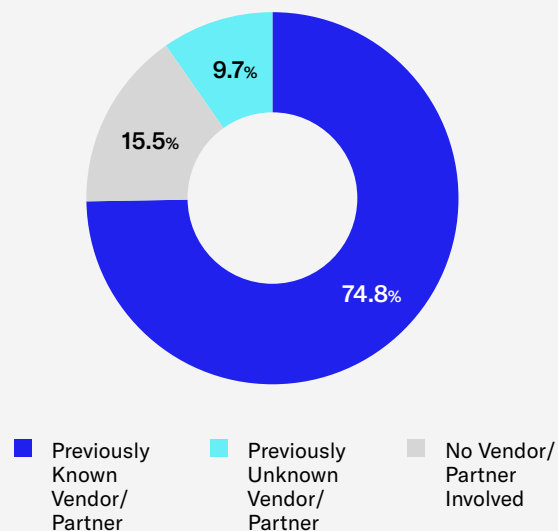


Figure 13: Threat Actor Redirects Funds from a Vendor or Partner Owed to a Business



## 75% of Financial Fraud Incidents Involve a Previously Known Vendor or Partner

Figure 14: % of Financial Fraud Involving a Known or Unknown Vendor or Partner



Only about 10% of financial fraud incidents occur with a previously unknown vendor or partner. The majority of financial fraud incidents occur with a vendor or partner the business already has a relationship with, representing nearly 75% of cases.

While much attention is often given to assessing and mitigating risks during the new vendor onboarding process, it is essential for organizations to conduct regular reviews and assessments of their ongoing vendor relationships to ensure that security measures and processes remain effective.

Companies must be vigilant about their interactions with known vendors, putting in place systems and procedures to verify the authenticity of financial transaction information before authorizing payment, especially when changes are requested.

## The Rise of Business Email Compromise

Business email compromise (BEC) is a cyberattack where a threat actor hacks into a victim's email. While the term financial fraud may sound like the result of a simple social engineering scam where a human is deceived into authorizing a mistaken transaction, the reality is 64% of financial fraud cases begin with a sophisticated hack into a user's inbox.

Once a threat actor has control of an email account, they are able to perform in-depth research on the hacked individual, their company, and its third-party vendor relationships to identify an opportunity to intercept a financial transaction. Once that opportunity is found, the threat actor will use the hacked email account to communicate with the third-party vendor to discuss transaction details, diverting communications away from the user's inbox in order to remain hidden.

This makes BEC tactics particularly effective. With full access to a victim's email account, threat actors craft a high quality scheme that is almost impossible to identify as suspicious. Communications come from a legitimate email account from a known entity discussing a transaction that is already expected.

Here is a step-by-step fictitious example of how a BEC financial fraud attack might unfold:

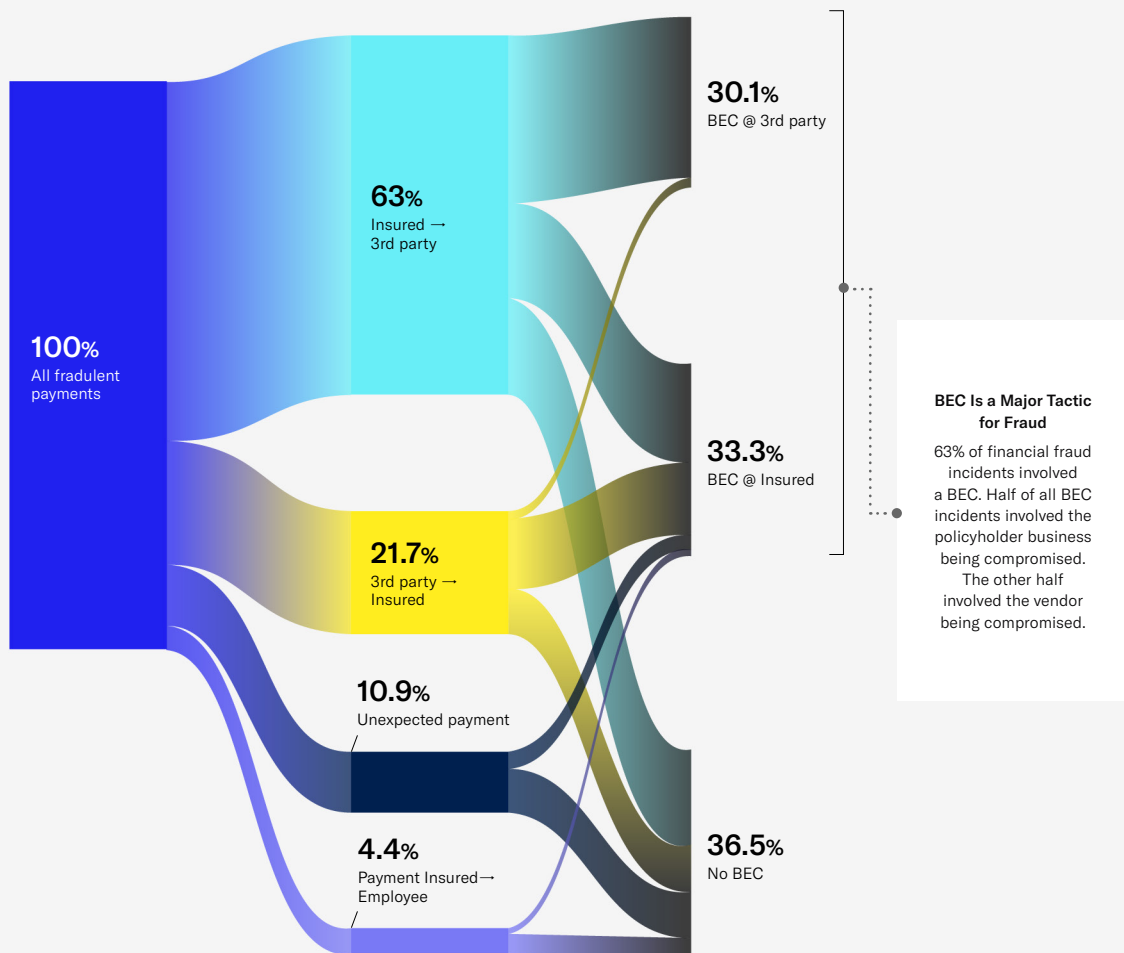
- 1 An attacker hacks into the inbox of the CFO at Ellison Metals and sees an expected payment from Exita Inc. for \$100K.
- 2 The attacker sets up a fake email address (CFO@elisonmetals.com vs. CFO@ellisonmetals.com).
- 3 The attacker sets up inbox rules in the CFO's mailbox to hide communication. Emails from pay@exita.inc skip the CFO's inbox and are sent to the trash.
- 4 The attacker sends an email from CFO@ellisonmetals.com to pay@exita.inc with cc: CFO@elisonmetals.com asking to change the ACH account number where payment is being requested.
- 5 When Exita Inc. responds, the email skips the CFO's inbox because of the inbox rules previously set, and the attacker receives the email in their spoofed inbox CFO@elisonmetals.com where they continue to communicate with Exita Inc. and request payment.
- 6 Exita Inc., believing the communication to be legitimate, processes the payment as instructed.

## Business Email Compromise: A Pervasive Financial Fraud Threat

In our data, about half of BEC incidents involve the insured business being compromised while the other half involves a vendor or partner of the business being compromised, meaning a vendor communication that appears legitimate could be compromised without the business even knowing it.

This underscores the importance of validating the legitimacy of the communication by other means beyond email. For any significant transaction, call the vendor to verify the authenticity of the request and all of the key details (account numbers, routing numbers, etc...) required to make the transaction.

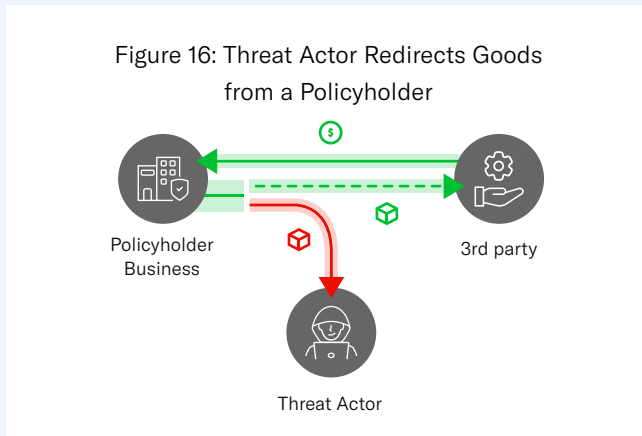
Figure 15: Business Email Compromise Accounted for 63% of Financial Fraud Incidents



Source: At-Bay Claims and Cybercrime Data, 2024 InsurSec Rankings Report

### VANISHING ACT: WHEN GOODS GO MISSING

A third less common financial fraud scenario (accounting for 4.5% of our 2023 financial fraud claims) involves stolen goods. Financial fraud is often thought of as a fraudulent wire transfer or payment of some kind, and this is typically the case. However, our research shows threat actors aren't just after cash – they're also fraudulently redirecting goods without payment.



Some real-world examples from our claims data include:

**\$206K**

worth of Christmas decorations

**\$59K**

worth of non-evaporated milk

**\$60K**

worth of paper towels

**\$196K**

worth of beauty products

In these cases, an order was placed by a threat actor and the goods were delivered to a physical location and then disappeared without the business being paid. What the criminals do with \$206K worth of Christmas decorations isn't certain, but the assumption is that the stolen goods would be sold for profit, conjuring striking similarities to more traditional organized crime – only without the breaking and entering.

While these types of thefts may require more onshore resources and coordination (fraudulent money schemes don't necessarily require people on the ground in the country where the theft happens), they are nonetheless lucrative.

With the proliferation of wire transfer fraud, organizations are learning to elevate security measures around cash transfers, such as know your customer (KYC) and better identity validation processes. However, we believe it's also important to extend the same security measures to the transfer of goods and services, especially when it comes to new vendors.

# Conclusion

Email attacks, especially financial fraud, continue to be both widespread and devastating for businesses. Yet we know email is critical to business communication and daily operations, so simply restricting email to reduce risk just isn't feasible.

We've shown in this report that those companies using specific email solutions (Google Workspace) and certain secure email gateways (Mimecast and Proofpoint) experience better outcomes than others. This is not a technical analysis of the theoretical ability of any given solution to thwart cyberattacks. This is an analysis using real-world claims data to understand the outcomes our customers using these products experience. Given the size of our portfolio and the scope of this research, we have found a statistically significant difference in those outcomes, which we believe is an important factor when considering which solution is right for your business.

Beyond platform selection, implementation, configuration, and maintenance play a large role in keeping a business secure. While we have not yet seen MX misconfigurations as a driver of claims, their prevalence in our portfolio is a security concern that we are actively addressing. We believe it is only a matter of time before cyberattackers target these vulnerabilities.

Similarly, this is why we continue to recommend cloud-based solutions, especially for small- and medium-sized businesses that typically do not have the IT resources to manage and maintain on-premises email platforms or security solutions. Cloud service providers monitor and respond to security threats related to their own infrastructure, pushing updates and patches through the cloud, rather than shifting that responsibility onto the customer's IT team.


Few small- and medium-sized businesses are equipped to maintain complex software on their own, and they can't afford to leave it to chance. The average financial fraud incident, which most often uses email as an attack vector, can cost nearly a quarter million dollars. To complicate matters further, a significant portion of financial fraud incidents begin with a third-party vendor or partner being impersonated or compromised. Investing in proper security tooling is important, and putting employee training and processes in place to identify suspicious emails from a vendor or partner is equally so.

Should the worst happen and a business is hit by financial fraud, there are ways to recover the money. Timing is critical. The faster the incident is reported, the faster both the sending and receiving banks of a wire transfer can be alerted, giving them a higher chance of either stopping the transfer or recovering the funds. Cyber insurance providers can help put the right processes in motion.

Over the period of this report (January 2023 through the first half of 2024), At-Bay helped policyholders recover over \$61M in stolen funds from financial fraud, including over \$33M in the first half of 2024 alone — but we believe there is more to do. Education and awareness driven by real-world cybercrime data analysis, like this report, are part of this continued effort to equip businesses with the insights they need to stay secure. Using this data to help close the security gaps, whether it's through coverage or security products, is another.

This is the power of InsurSec: a closed-loop system that uses real-world cyber insurance claims data to inform security recommendations and deliver end-to-end prevention and protection for safer businesses. It's the way cyber protection should be.

Sharing these analyses also benefits the security apparatus at large by providing insights and intelligence that can be used to inform the development of more robust and effective cybersecurity tools and measures across industries, contributing to a more resilient and proactive cybersecurity ecosystem.



At-Bay helped policyholders recover **\$33M** from financial fraud schemes in the first half of 2024.



# Methodology

At-Bay’s analysis is based on claims information from 2021 through the first half of 2024. Incidents reviewed included those related to email claims and financial fraud. By analyzing actual claims data, the At-Bay Research Team set out to answer these questions:

- How are email-related attacks changing?
- How do outcomes associated with specific email solutions and email security solutions differ?
- How do financial fraud attacks occur?
- How does financial fraud impact businesses?

This data was collected from At-Bay policyholders during initial underwriting, throughout the policy year, as well as when their claims were processed by our team in the wake of an incident.

To establish the set of “Email Security Solutions” that were worth investigating, we identified more than a dozen providers that were prevalent enough within our customer population to warrant further analysis. For the selected solutions, our researchers established a normalized claims frequency to identify potential correlations with incident occurrences. After further analysis, six email security solutions were considered prevalent enough to provide statistically significant results. The same was done for the “Email Solution” category.

By identifying the solutions that have a high or low claims frequency compared to the average, we believe that we can assess the relative effectiveness of email security solutions in mitigating the risk of security incidents stemming from email usage.

We infer from this that the email security solutions which appear less frequently in our dataset are more effective at mitigating email risk. The same goes for the customers who didn’t have an email security solution in place, that the relative claims frequency is indicative of the effectiveness of the native security capabilities that come built-in for today’s email solutions.



## ABOUT AT-BAY AND THIS REPORT

At-Bay is the InsurSec provider for the digital age, helping businesses mitigate cyber risk and avoid incidents by continuously analyzing data from security scans and collecting cyber threat intelligence and the relevant details of security incidents reported by insureds. Because we can correlate information about a significant number of real-world incidents with data about the victim's technology environment before the incident occurred, this enables us to reliably identify trends and relationships that other companies and security vendors cannot. We're able to clearly identify security controls that mitigate risk, differentiate them from security controls that don't mitigate risk, and prove our case with empirical data from actual incidents where those security controls were in place.

Our goal is to share our findings on the respective impacts of a range of security controls with the public at large. We believe we can use facts and evidence to cut through the noise of a crowded cybersecurity marketplace and enable organizations to deploy scarce cybersecurity resources for maximum impact. We regularly develop and share a slate of statistically provable leading practices for security that can be readily consumed by organizations regardless of headcount or the size of their security budget.

This document is intended for information purposes only and does not modify or invalidate any of the provisions, exclusions, terms or conditions of the policy and endorsements. For specific terms and conditions, please refer to the coverage form.

At-Bay Insurance Services LLC is a licensed insurance agency and surplus lines broker in all fifty states and the District of Columbia.  
©11/2024 At-Bay. All Rights Reserved.

at  
— bay