Underwritten by

Bottomline

Written & Produced by

Strategic Treasurer

TREASURY FRAUD & CONTROL

Survey Report

2022

Exclusive Report

- Fraud Experiences & Exposures
- Security Controls & Spend
- Fraud Detection & Prevention

Contents

SURVEY CONTACTS

Craig Jeffery, FLMI, CCM
Founder & Managing Partner
craig@strategictreasurer.com

Brian Cochrum
Director of Marketing
brian@strategictreasurer.com

Kylene Casanova
Marketing Manager
ky@strategictreasurer.com

Survey Quick Stats

230+ respondents

100+ questions

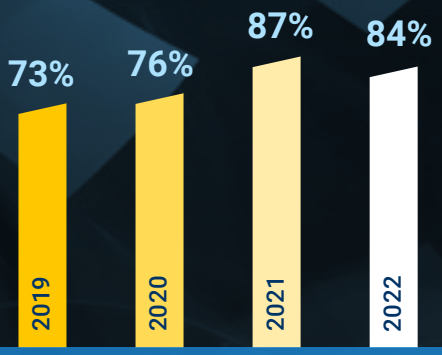
9-week survey runtime

7th year of research

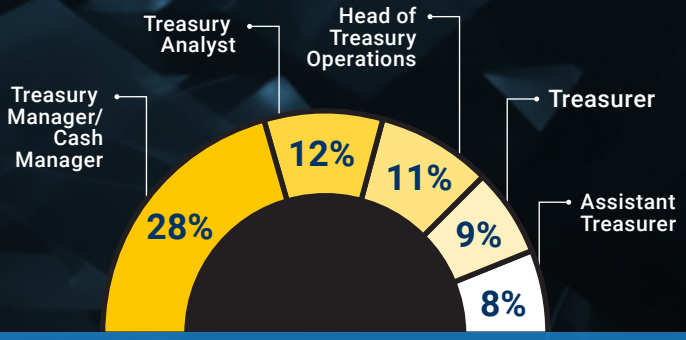
DEVELOPMENT | **RUN TIME** | **ANALYSIS**

September	October	November	December	January	February	March

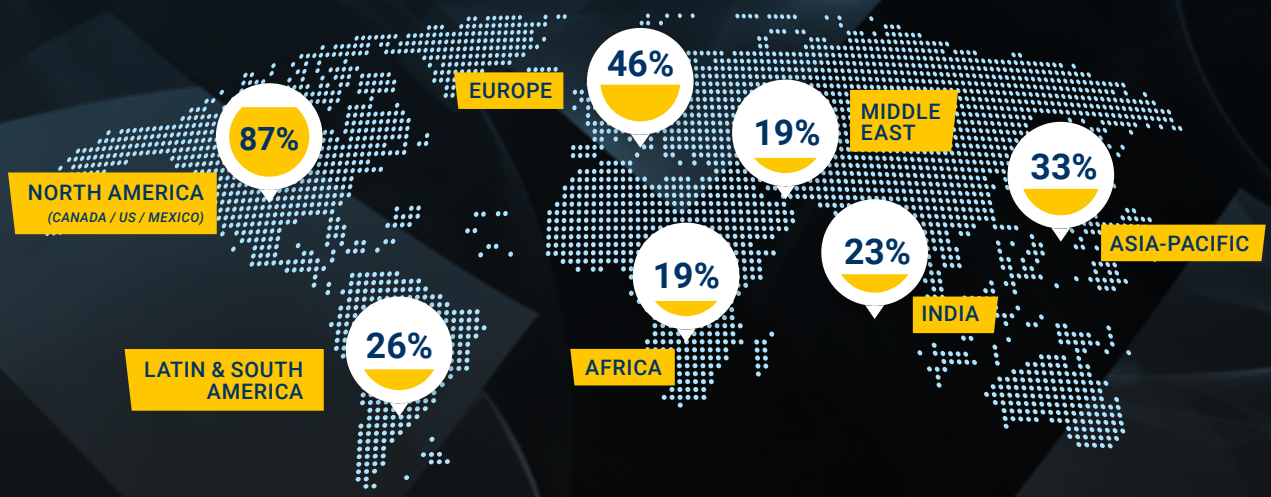
Fraud Increase Over the Years



Top Corporate Roles



Respondent Regions of Operations



Executive Summary

This is the 7th annual edition of the Treasury Fraud & Controls Survey underwritten by Bottomline and written and produced by Strategic Treasurer. 230+ finance and treasury professionals from corporations and banks around the world participated in this comprehensive survey sharing their thoughts and practices across many areas.

For those who either remember broken records or those that have watched a video of what a broken record does, there are a few places where this report seems to be a repeat of last year and perhaps the year before. This is certainly true in some areas. The seriousness of fraud and the view that the criminals perpetrating these attacks and the companies suffering losses is quite real. We think the "skipping" of the record in these cases is instructive in that the pain and issue hasn't gone away. Importantly, the same tune is played at a higher volume in some cases. Examine the four-year upward trend of respondents indicating a significantly more serious threat of fraud. The trend is useful information, and the increase in volume is an appropriate alarm.

The shift to working from home (WFH) is causing many companies to explore how the location of workers may increase the threat level, and their responses allow us insight into what they are doing in order to mitigate this risk.

Banks seem to have been more diligent in their defenses since they appear to be performing better at preventing and detecting fraud than their corporate peers. There are several practices that show correlation with lower losses, and banks are outpacing corporates here too. Strengthening the "human firewall" through training and testing is one such area where we see correlation.

Faster Fraud.

Sixty-two percent of respondents see the shift to RTP as a risk, speed being the top concern, followed by the rules and newness of these platforms.

Monitoring.

One-third of companies use monitoring methods that detect potential fraud before payments are out the door. Prevention is superior to detection.

Continued Risks of WFH.

With a deeper reliance on remote work, banks are experiencing a larger impact of risk exposure on internal factors. Four of the top six factors include increased risk exposure—directly or indirectly, intentional or not—resulting from employees' actions.

CRAIG JEFFERY, FLMI, CCM
Founder & Managing Partner
Strategic Treasurer

OMRI KLETTER
Global VP, Fraud & Risk Management
Bottomline

CHRISTOPHER GERDA
Risk & Fraud Prevention Officer
Bottomline

Business Email Compromise (BEC) Remains the Top Driver for Fraud Exposure.

Eighty-seven percent of banks and 73% of corporates perceive BEC as the highest risk over the next 12-24 months.

Investigating Financial Crimes Takes a Front Seat.

Sixty-seven percent of respondents indicated their plans to use network visualizations and analytics as part of their strategies to investigate financial crimes. **Visualization** is a superior method for identifying attack activities after the fact compared to audit trail information.

Fraud Controls.

Eighty-eight percent indicated data security and 78% indicated employee education as current controls in place to prevent fraud. Eighty-five percent of respondents indicated that AP and AR are key areas for bolstering fraud prevention and control investments.

Thank you for taking the time to read through this information. For those who took the rather lengthy survey, thank you for your time and for helping out the industry. This input allows us to understand what is happening and what professionals are thinking and doing. Accordingly, we can then better understand the world of fraud based upon massive amounts of data rather than on limited knowledge from our direct exposure to this fraud.

Enjoy the read.

CORPORATE

BANKS

Within the following pages, these icons indicate whether the questions were asked of corporate respondents, bank respondents, or both within the survey's branching logic.

Additional resources related to this survey:

- *Infographic report*
- *Webinar replay*

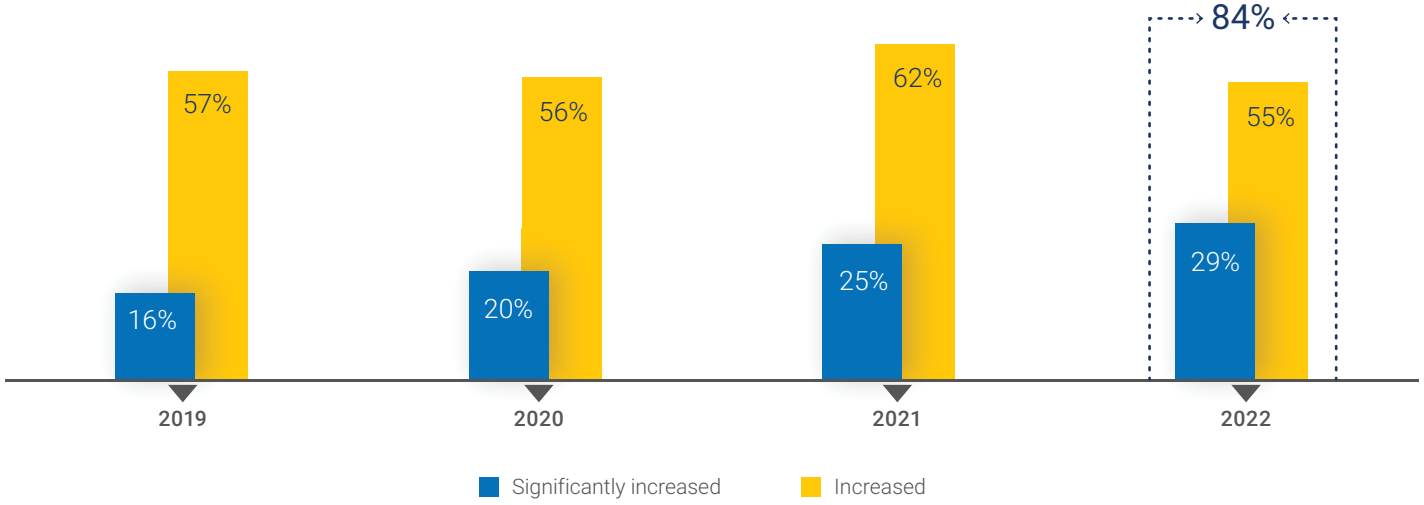
Key Finding Analysis

Comfort with security posture still comes with increasing concerns

The percentage of companies indicating that there is a significant increase in the threat level has expanded over the past four years. Twenty-nine percent of firms are now reporting this increase in severity. Concurrently, over half (59%) of respondents indicated that they believe their company is in a better net position with regards to their defensive posture and the threat they face.

- Twenty-nine percent have noted a significant uptick in significant threat. This escalation has expanded: 16% » 20% » 25% » 29% from the 2019 survey to the current one in 2022.
- **The majority believe they are in a better position in a deteriorating environment**. Fifty-nine percent of respondents believe they are in a better or significantly better position on the security front as compared to last year. The majority of respondents believe that they are in a good position despite the uptick in the seriousness of the threat.

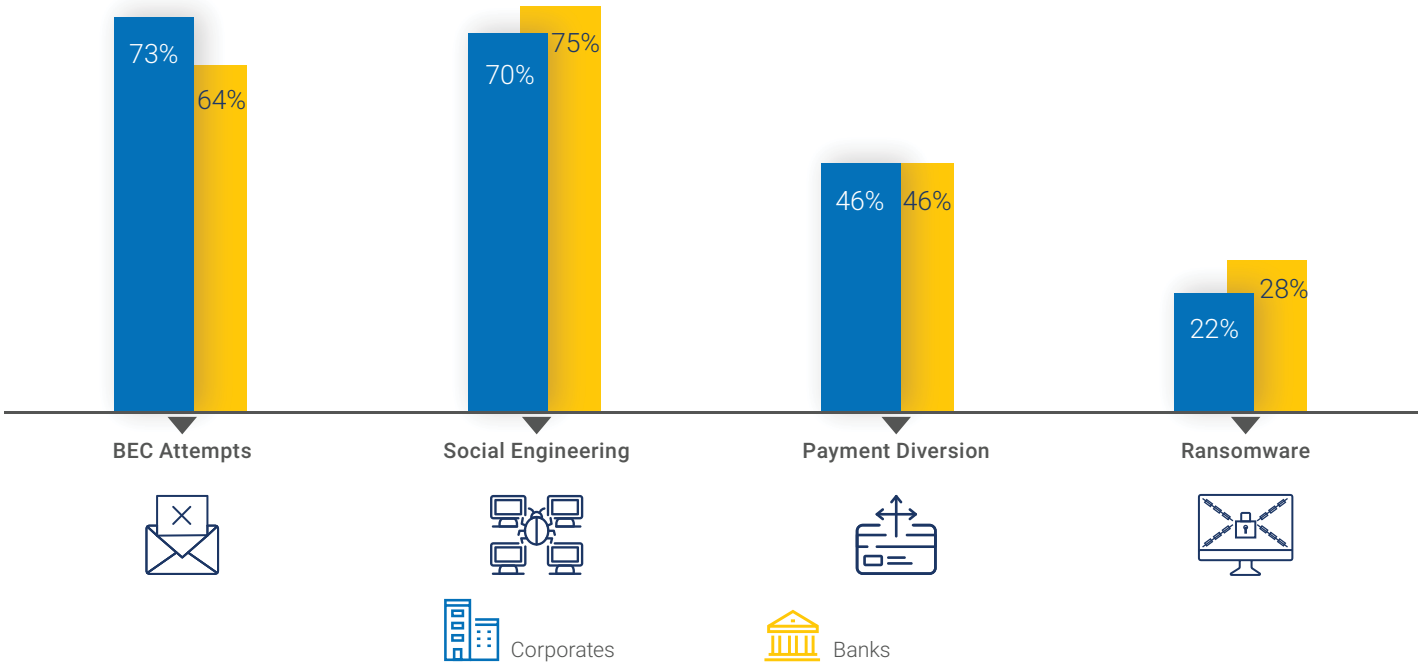
In the past year, I think that the threat level of fraud has:



Nature of work has increased fraud exposures, but banks seem to be outpacing their corporate counterparts

With many companies still in the work from home (WFH) environment, it is concerning that the work location was identified with higher attempts at fraud or fraud attacks that ended in a loss. Just over three in four firms (78%) noted this, with BEC and social engineering attacks making up the majority of the fraud attacks.

The details behind this cover several significant fraud types:



CONSIDER

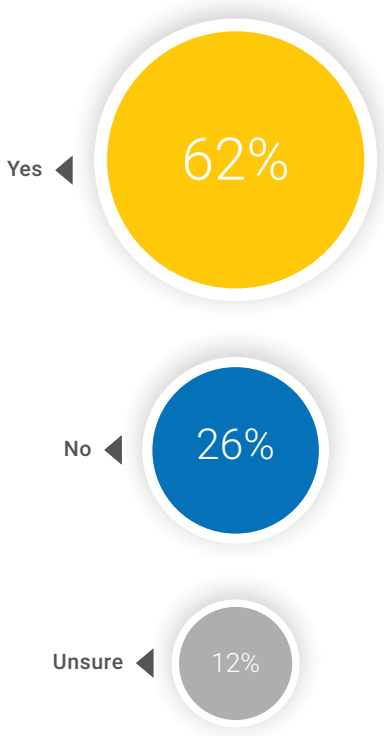
Virtually no banks indicated that they had suffered losses from BEC, social engineering, etc., suggesting possibly that education within these highly regulated, compliance-driven organizations have had an effect in stopping damage from forms of fraud that their corporate customers still suffer. If banks are doing a good job with awareness and education, it is reasonable to suggest that corporate payment professionals should understand what banks are doing and what they are telling their clients.

Concerns that faster payments will lead to more fraud losses

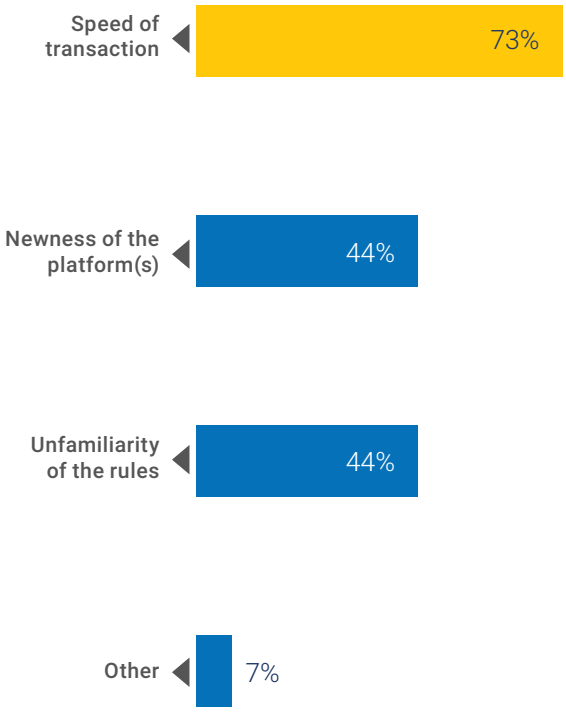
The data shows that most companies have concerns that faster or real-time payments add potential risk into the payment processes. Two key drivers for this response have to do with the speed of the transactions and the relative newness of these faster payment platforms.

- Sixty-two percent see the shift to faster or real-time payments as a potential risk.
- Speed is the top reason given for this risk (73%).
- Rules and newness of real-time payment platforms are identified by 4 out 9 respondents.

Do you see the shift to faster / real time payments as a potential risk?



The potential risk is related to: (Select all that apply)



AP/AR and treasury biggest recipients of fraud prevention spending

Your peers involved in payments are highly likely to be spending more on fraud prevention, detection, and controls. Accounts payable and accounts receivable (85%) and treasury (70%) are all cracking open their digital wallets to better protect their payment processes. Naturally, their spending is also targeted at the higher fraud-frequency areas of exposure (BEC, transaction fraud, etc.).

- AP/AR (85%) and treasury (70%) are the payment areas where companies plan to spend more on fraud prevention, detection, and controls.
- This tremendously outpaces areas like payroll (26%).

The following represent areas where more is being spent for protection:

BUSINESS EMAIL COMPROMISE (BEC) ▸ **59%**

BANK TRANSACTION FRAUD ▸ **52%**

TRANSACTION CONTROLS ▸ **48%**

BANK RECONCILIATION ▸ **37%**

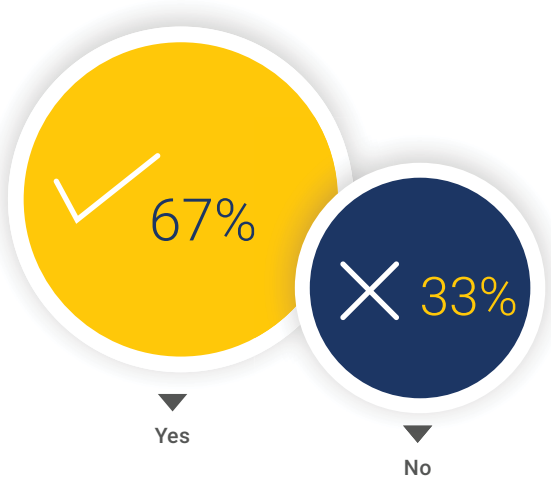
SYSTEM ASSESS ▸ **37%**

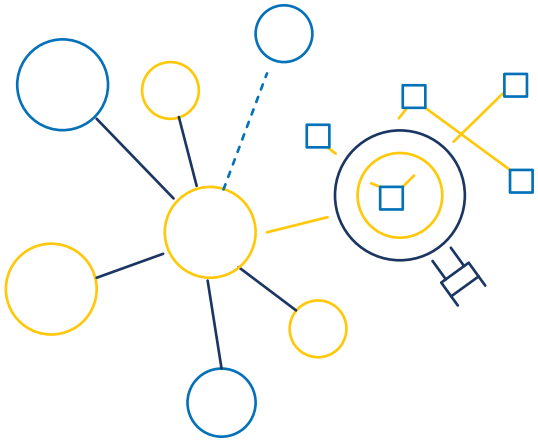
Visualizing financial crime

If the maxim "what gets measured gets improved" is correct, then perhaps what is visualized gets better protection. Two-thirds of organizations are using or plan to use network visualization and analytics to investigate financial crime. This represents a significant increase in capabilities over the traditional "audit trail" process that companies have been accustomed to using to determine what went wrong in a fraud situation.

- Sixty-seven percent of companies have plans to use or consider the use of network visualization and analytics as part of their strategy to investigate financial crime.
- Firms see greater value of visualization in identifying attack activities during and after the fact as compared to simply capturing audit trail information.

Do you have any plans to consider the use of network visualizations and analytics as part of your overall strategy of investigating financial crime?

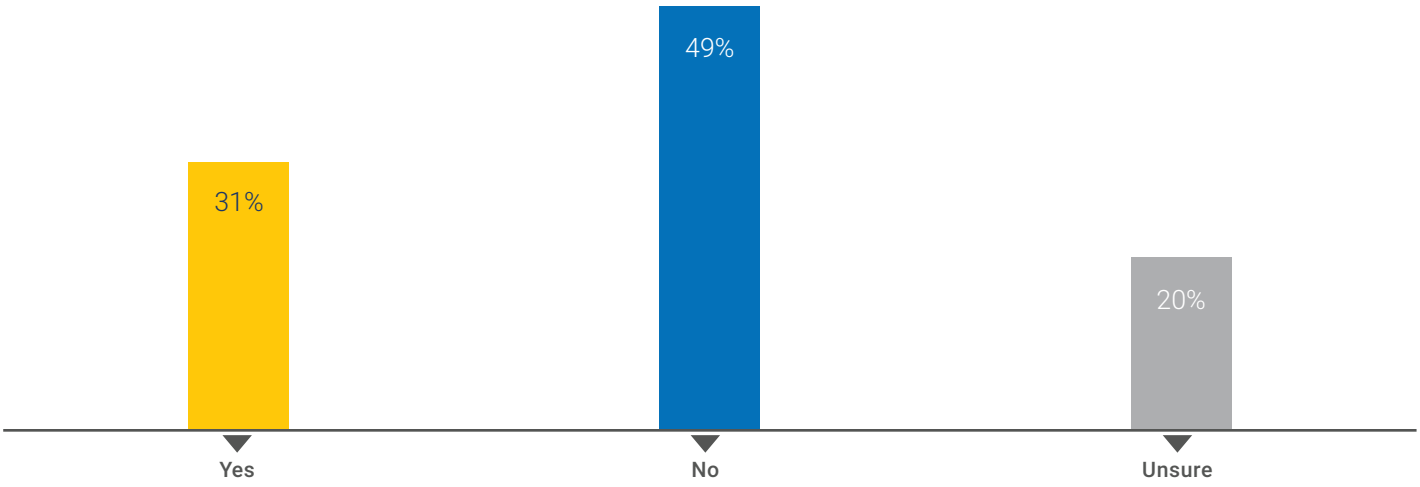




More work left to be done before fraud

Only 1/3rd of finance groups use payment monitoring to detect potential fraud before payments are out the door. We expect to see continued and more rapid growth of prevention and early detection services being employed over the coming years.

Do you utilize a payment monitoring solution that will detect potentially fraudulent payments BEFORE they leave the building?

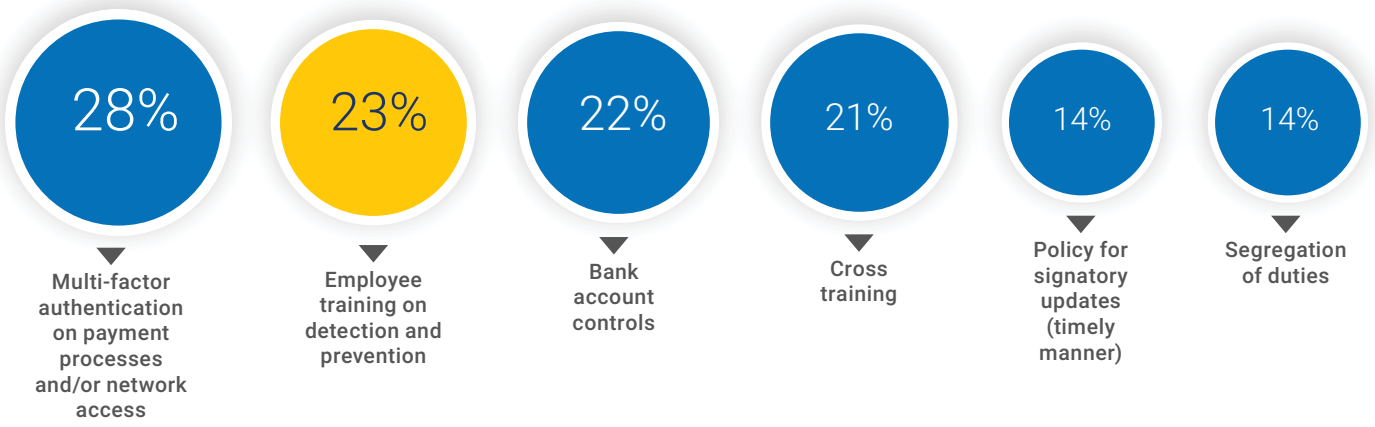


Bank security services adoption

Banks have been encouraging corporates and the world at large to adopt bank security services. Beyond offering direct services that prevent or detect fraud, they are also underscoring their emphasis on safety and security with the delivery of security education or training for their customers. Banks are pushing their clients hard in an attempt to increase the uptake of services, understanding, and training. Has this advocacy borne results? We argue that since banks have been the most consistent and vocal in pushing for the use of security services, education, and training, they are responsible for the encouraging movement in this area.

- Uptake: "Year of More"—23% employee training on detection and prevention (something banks have been encouraging for some time).

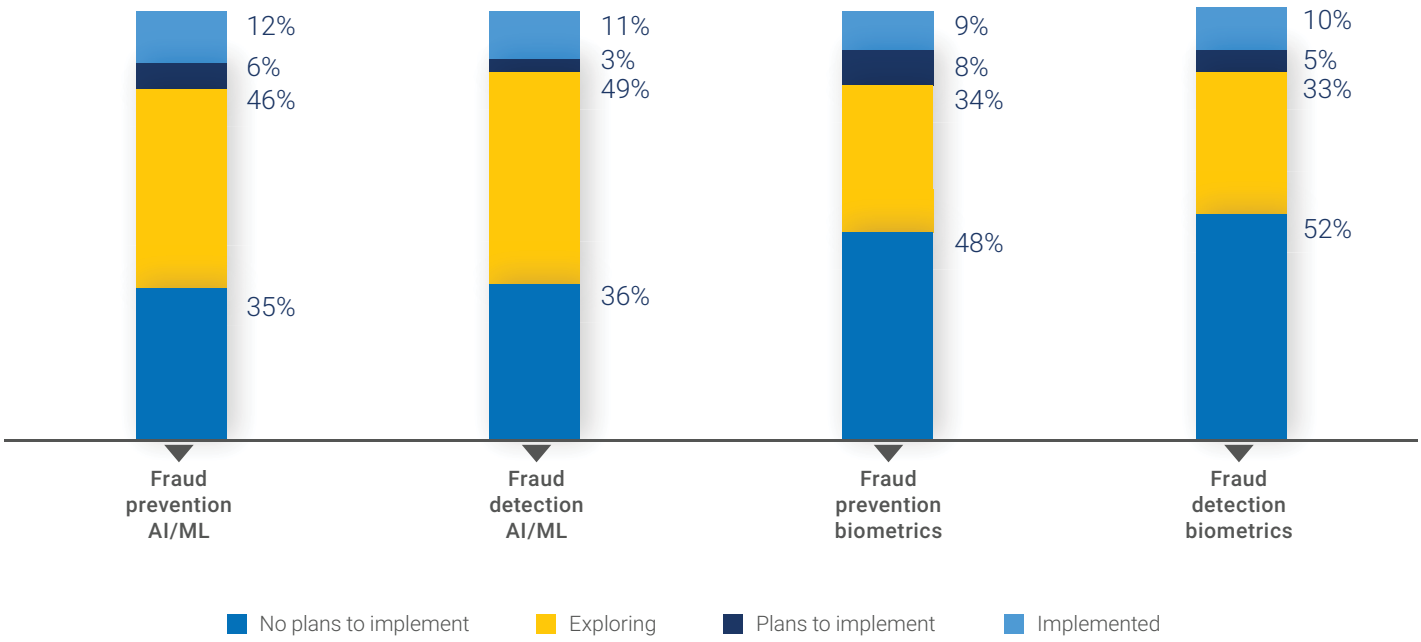
Of the controls you have in place, which have been added in the last year? (Select all that apply)



More saying YES to AI/ML in fraud detection & prevention

More than half of businesses are exploring, plan to implement, or HAVE implemented AI/ML technologies to detect and prevent fraud. AI/ML fraud prevention and detection has now passed the inflection point of adoption. However, more than 1/3rd have no plans to implement.

What is your position regarding adopting the following technologies?



Final Thoughts & Action Items

The following represent a mere handful of action items to consider and then implement as relevant. For those currently taking these steps—well done. For those who have much work to do, we encourage you to prioritize the list and put each of these elements on a roadmap for implementation. Getting something done every month or quarter is superior to making a huge list with an unreasonable timeframe that is missed.

Making consistent and steady progress will substantially improve your organizational defenses. Importantly, it will help your team understand the continual nature of the journey and avoid a "destination" outlook of security. We must continue on the journey and avoid believing that we have arrived and can stop to rest.

Sober and Concerned Attitude.

Your corporate peers have continued to be more concerned about the growing levels of year-over-year "significant increase" in the threat level. This concern is based upon experience. Many of your peers feel they are in a better position with regard to this acceleration of fraud and its attendant concerns. We suggest that the concerned attitude about the overall situation be coupled with sober reflection about your organization's overall position with regard to the threat. There is significant risk of being overconfident and only a minor risk if you underestimate your capabilities. Finally, to increase the somber attitude a bit more, even for those firms who are truly in a much-strengthened position now, if they don't continue to improve, they will quickly fall below the standard of control and protection they seek to achieve.

Assess Your Position.

You want a realistic view of your controls and security. There are several ways to get there. Figure out what you need to do and then act. Your organization may do one thing or everything, but do something.

- Have an independent (external) review of your payment processes.
- Benchmark your security processes, practices, and position compared to your peers.
- Do an internal review (self-assessment) of your control situation.
- Determine your action plan and move forward.

Get Trained and Tested: Strengthen the Human Element.

Upgrade staff with security training for payments. Firms where employees are trained on security experience lower loss levels by significant margins. This is one of the most obvious areas of focus for those who haven't made this a consistent practice.

Monitor the Situation of Fraud.

Monitor your systems and points of exposure as if your money and data depend upon it.

- Assign specific people to specific fraud types and areas of security. They should be accountable to the organization to understand what is going on externally and bring that knowledge inside your organization.
- Meet quarterly. Review issues and progress and update future plans.
- Ensure you have system-level monitoring to identify potential issues before information or funds have left your servers or banks. If you can add interdiction services (medium firms and larger) to stop suspected processes so that they must be reviewed, make that happen.

Change the Default Setting: Using Security Services.

Your banks and payment process providers offer security services and may be recommending them to your organization. They likely include some cost. These services need to be evaluated for applicability. Your default position when your bank or technology vendor offers services may be, "I won't buy until and unless I am fully convinced." This has probably served you and your company well in the past for any type of purchase. However, we invite you to take a different default position: "We will be generally in favor of security services and monitoring features unless it is obvious to us that they are not needed or we have better alternatives already in place."

Have a concern or need the answer to a question?

CONTACT AN EXPERT.

Bottomline
info@bottomline.com

Strategic Treasurer
info@strategictreasurer.com

Appendix

EXCLUSIVE REPORT

(Ambassadors & Respondents)

This next chapter of the report contains a subset of questions asked within the major sections of the 2022 Treasury Fraud & Controls Survey. While this information is not made available to the general public, for those individuals that completed the survey, we have provided additional data and analysis. This is intended as a token of appreciation for those who take the time to make our market research so valuable.

HOW CAN I ACCESS THE FULL RESULTS?

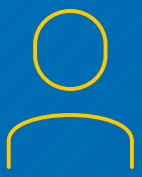
Although a significant amount of data is included in this appendix, we do not display the results from every question. However, individuals wishing for further analysis on any point of interest are encouraged to contact Strategic Treasurer for more information. Please reach out to Brian Cochrum at *Brian@strategictreasurer.com.*

CORPORATE

BANKS

Appendix Breakouts

Within the following pages, these icons indicate whether the questions were asked of corporate respondents, bank respondents, or both within the survey's branching logic.



SURVEY DEMOGRAPHICS

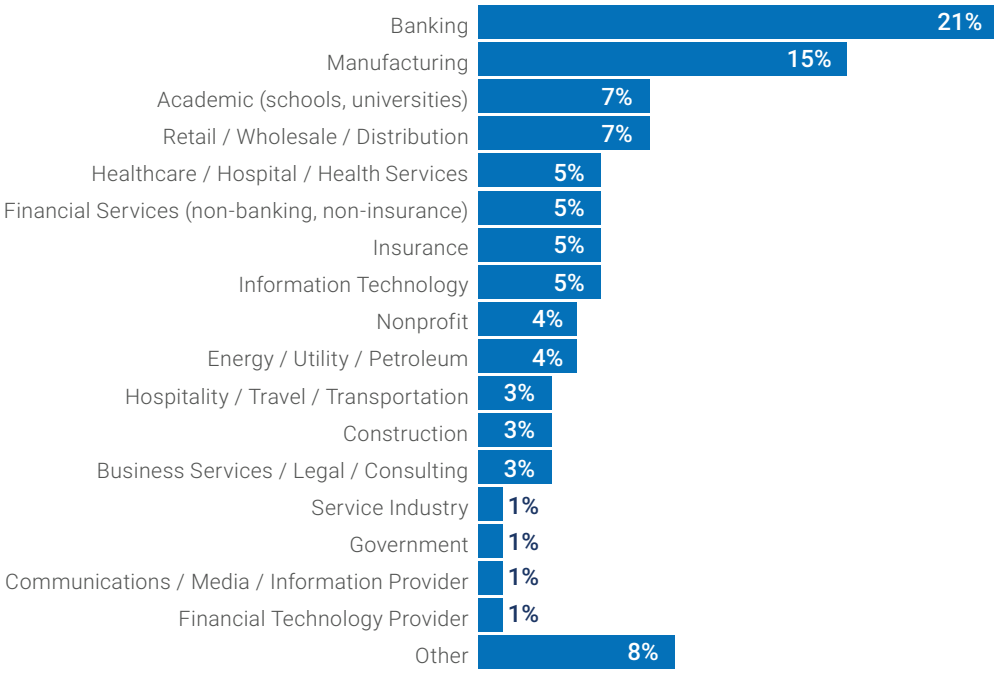
FRAUD EXPERIENCES & EXPOSURES

SECURITY CONTROLS & SPEND

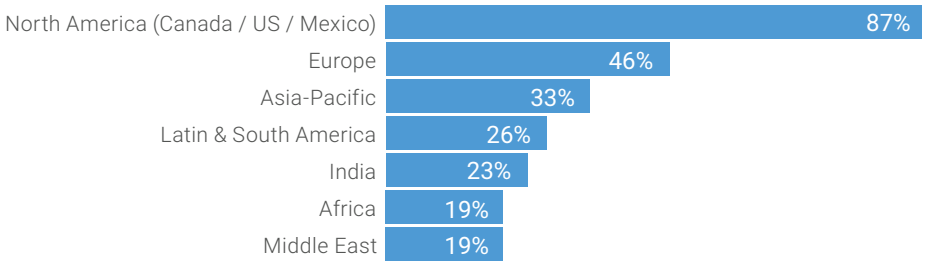
FRAUD DETECTION & PREVENTION

Demographics

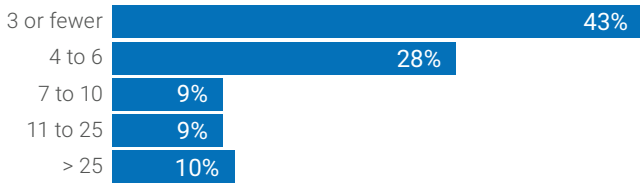
What is your organization's industry?



Which regions does your company operate in? (Select all that apply)

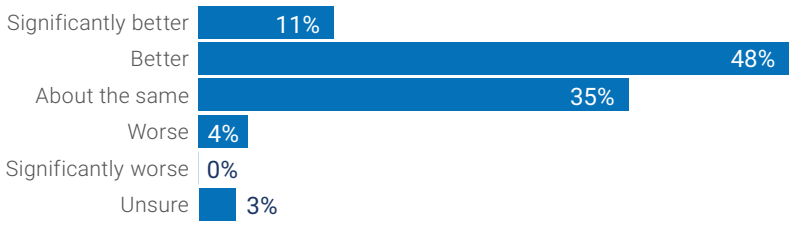


How large is your global treasury organization, including analysts?

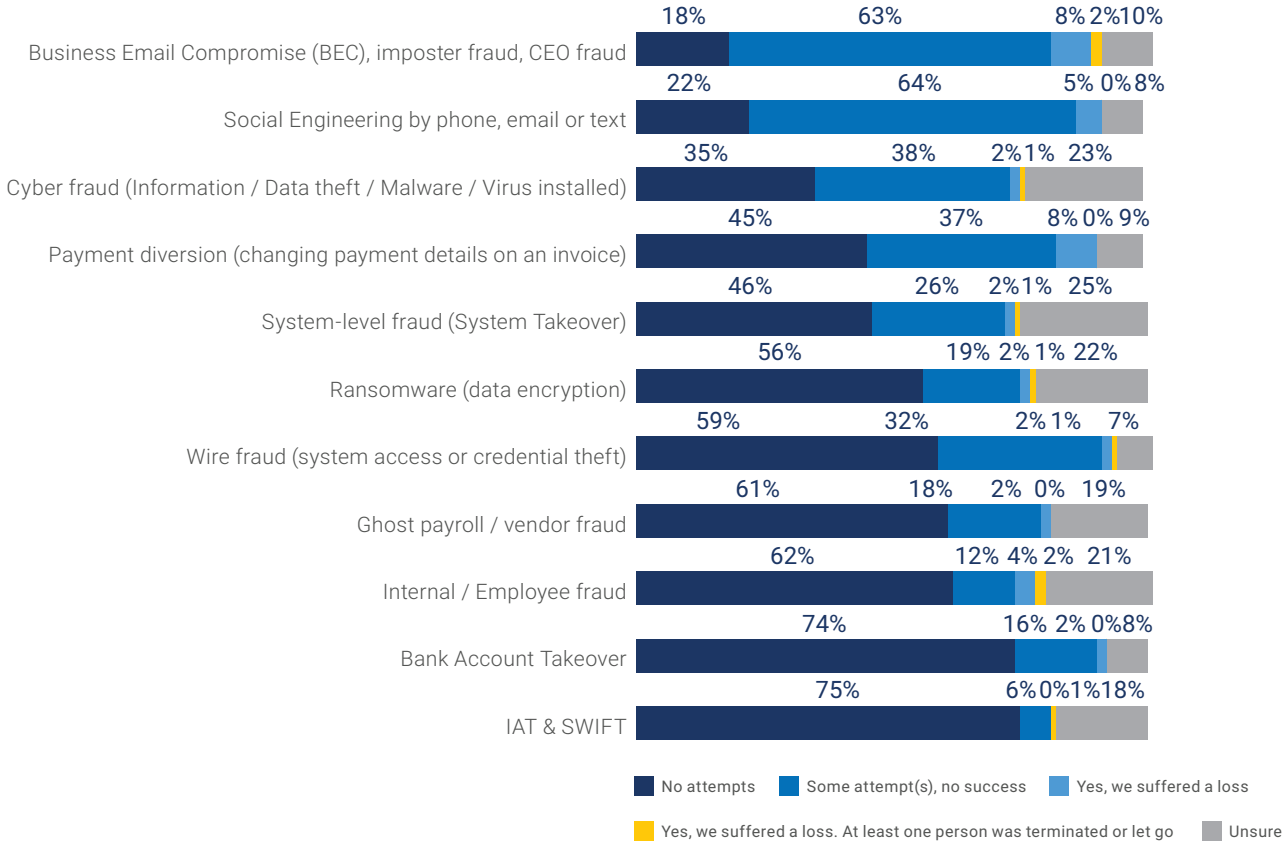


Fraud Experiences & Exposures

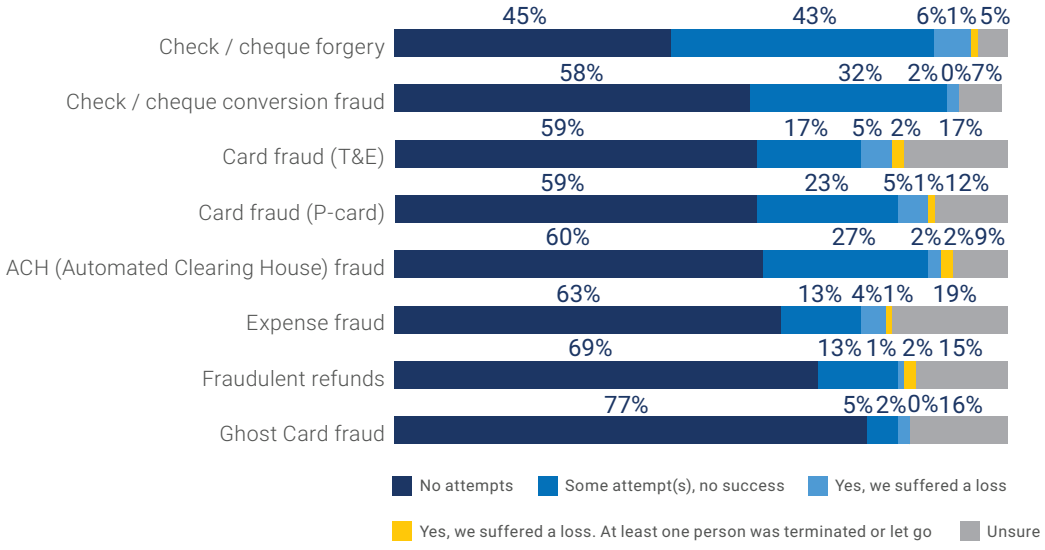
With regard to the threat level associated with fraud and considering our current security posture, we are in a(n) _____ position as compared to last year.



Thinking of the last 12 months, please label your company's experience with each of the following:

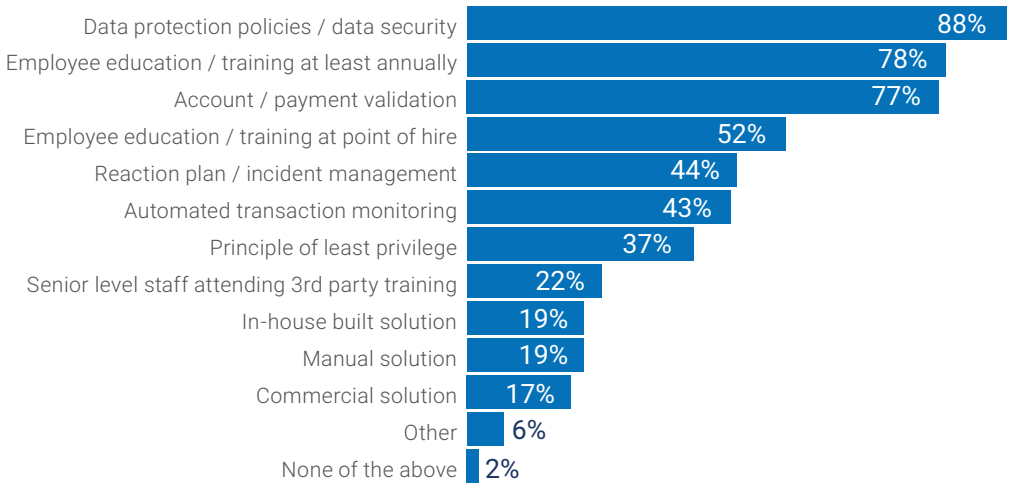


Thinking of the last 12 months, please label your company's experience with each of the following:

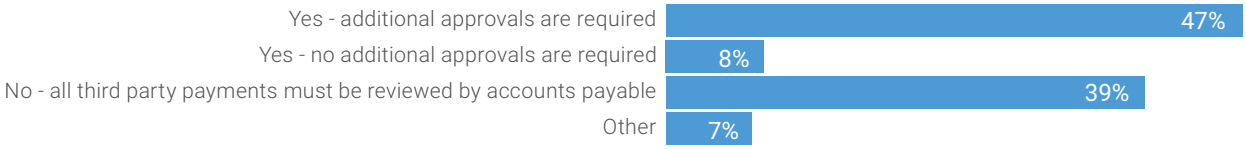


Security Controls & Spend

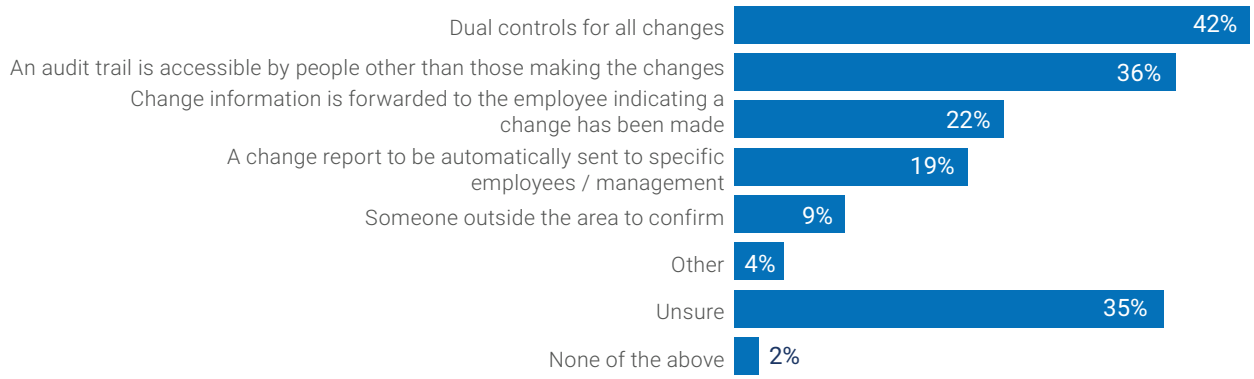
What controls do you have in place to prevent fraud? (Select all that apply)



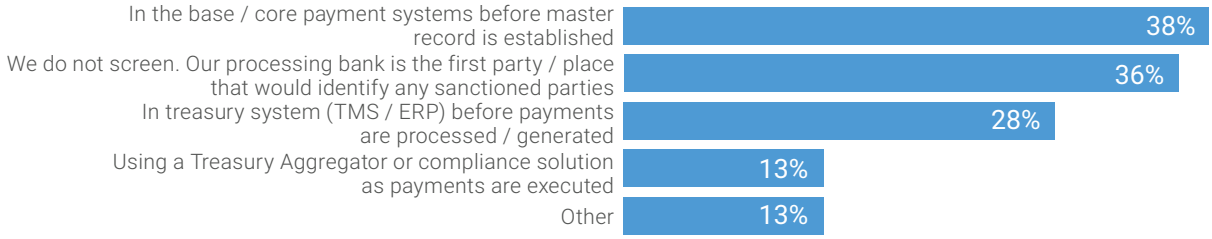
Does your organization allow wires to be processed to third party accounts which have not been processed by the accounts payable process?



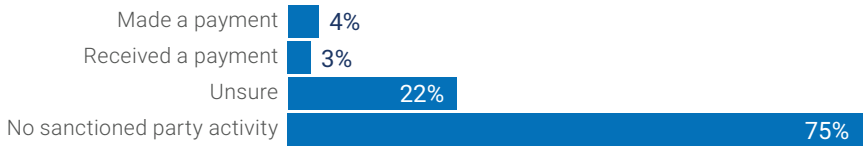
For master record changes on Employee (EE) records, we require: (Select all that apply)



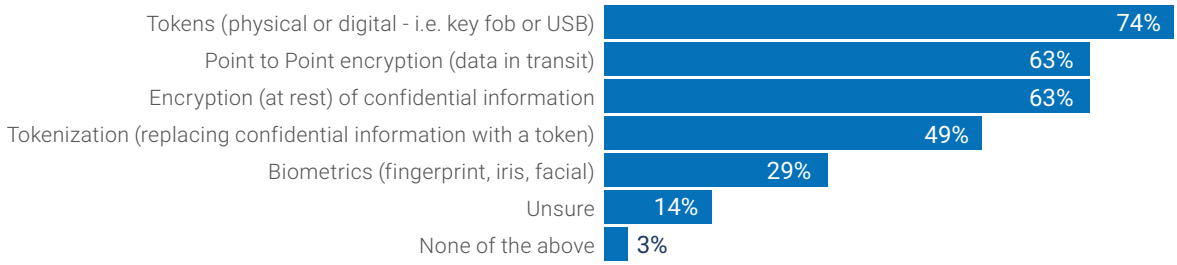
We screen for sanctioned parties: (Select all that apply)



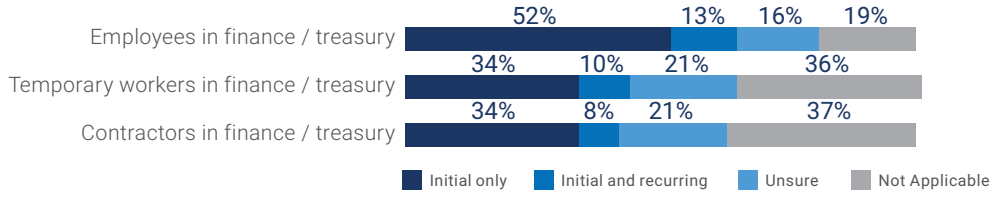
Have you inadvertently made a payment to or received a payment from a sanctioned party in the past 12 months? (Select all that apply)



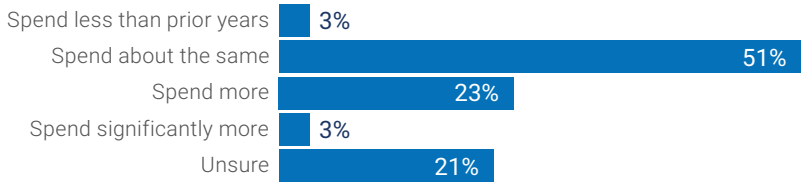
Are you using any of the following access or security methods: (Select all that apply)



Staff and Personnel. We perform background checks to include credit history:



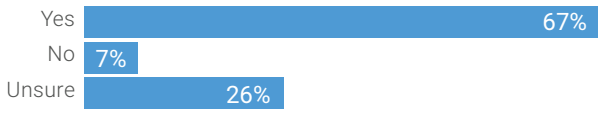
What are your spending plans for treasury fraud prevention, detection, and controls?



Fraud Detection & Prevention

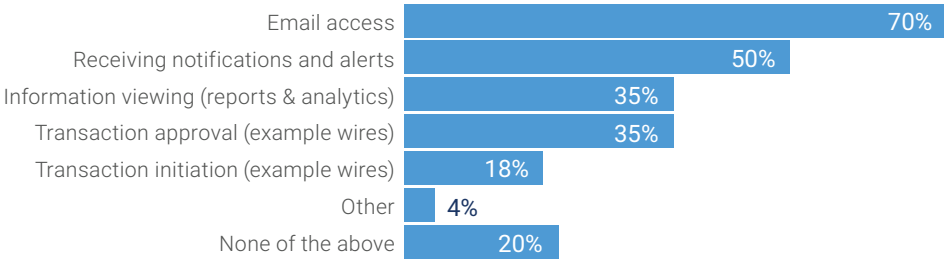
Does your organization have a centralized location where suspicious or fraudulent activity can be reported to a group who investigates it?

Does your organization utilize third party software to detect malicious emails seeking to download viruses/malware or containing phishing links to external websites?



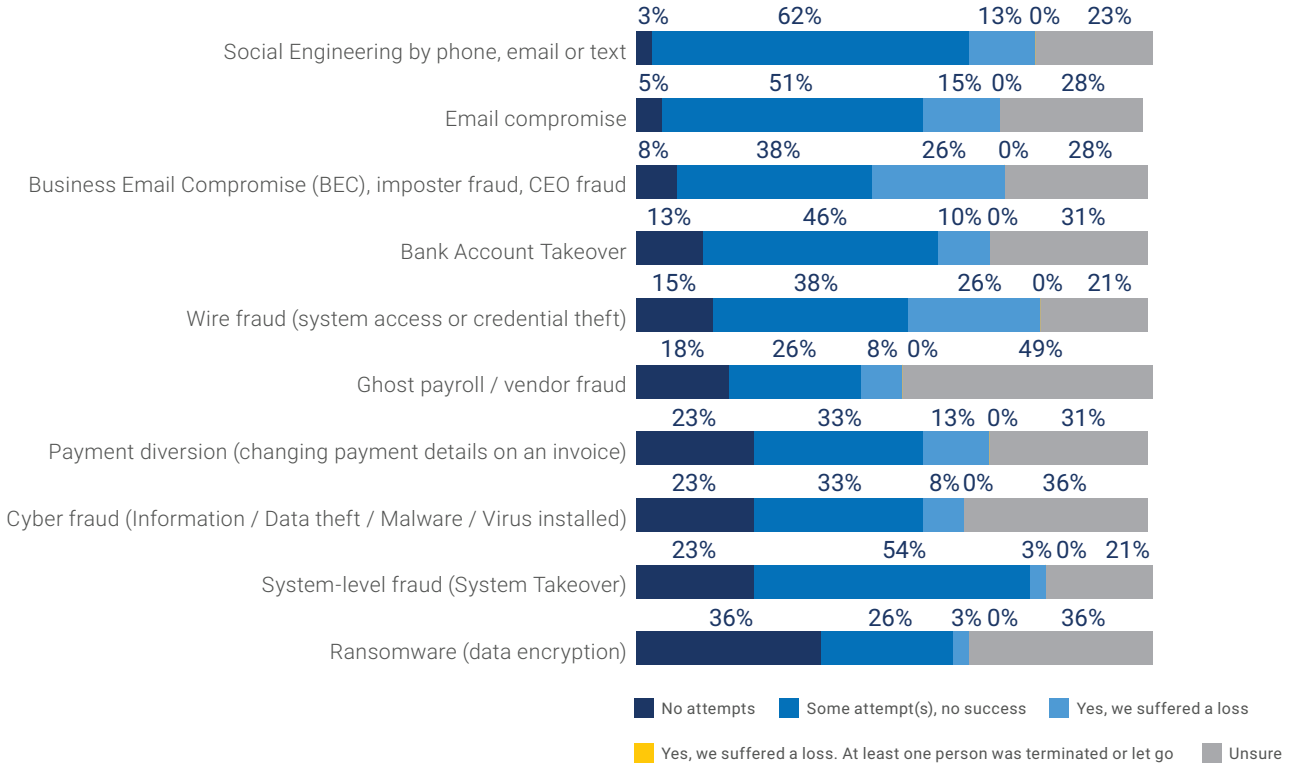
How often are your banking resolutions reviewed / updated?

Our company allows treasury to use their own mobile device for: (Select all that apply)

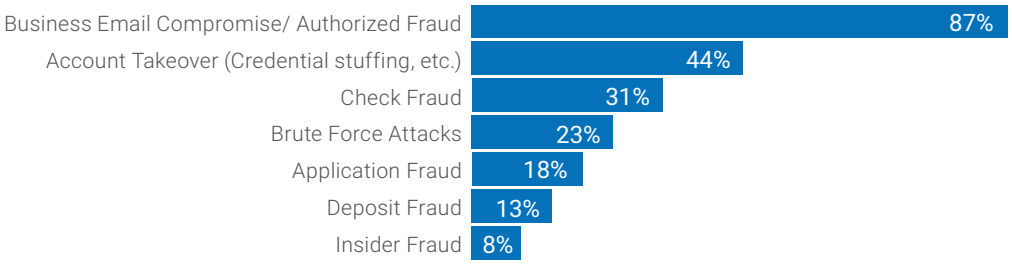


Survey - Bank Respondents

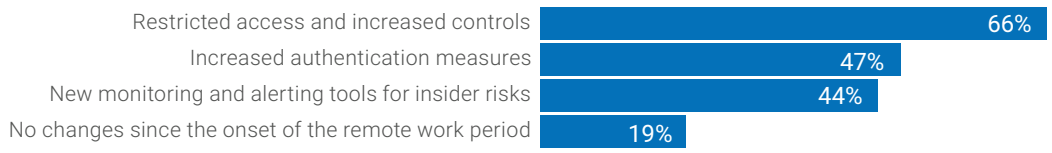
Thinking of the last 12 months, please label your company's experience with each of the following:



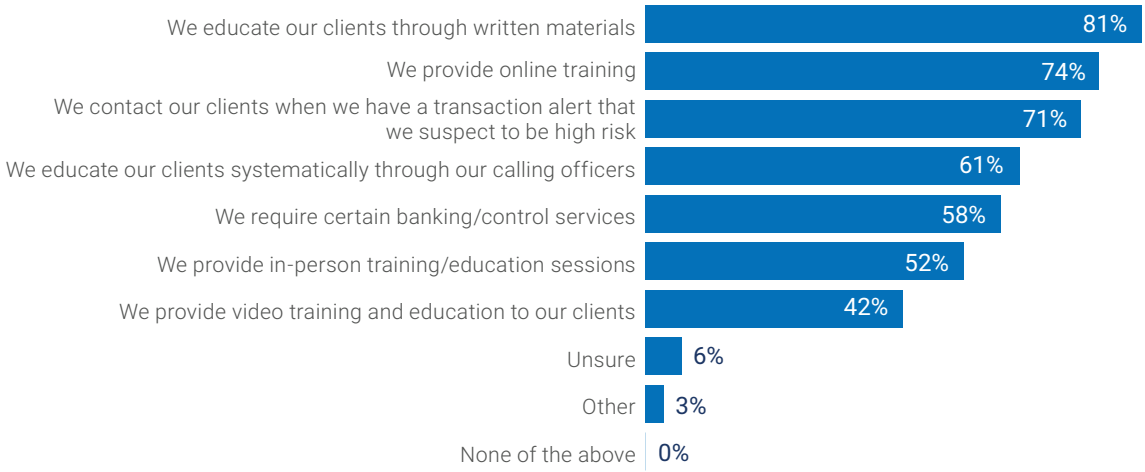
What do you perceive as your greatest fraud risk over the coming 12-24 months? (Select up to three)



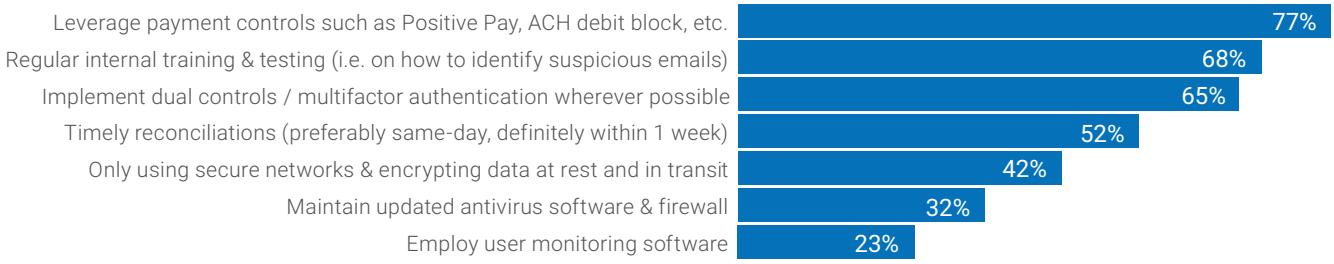
Remote work environments increase the risk of internal fraud, policy violations and brand reputation, what has your organization done to decrease its risk? (Select all that apply)



How do you help your corporate clients detect and prevent fraud?



What are the top three security practices or tools you wish all your clients used but that many are not currently leveraging?



About the Firms

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.

+1 800.243.2528 (US)
+44 118 925 8250 (EMEA)
bottomline.com
info@bottomline.com

Strategic Treasurer was founded in 2004 by Craig Jeffery, a financial expert and trusted advisor to executive treasury teams since the early 1990s. Partners and associates of Strategic Treasurer span North America and Europe.

This team of experienced treasury specialists are widely recognized and respected leaders in treasury. Known for their expertise in treasury technology, risk management, and working capital as well as other cash management and banking operations, they efficiently identify issues, creatively explore ideas and options, and provide effective solutions and implementations for their valued clients.

+1 678.466.2220
strategictreasurer.com
info@strategictreasurer.com

Bottomline

bottomline.com

STRATEGIC TREASURER

strategictreasurer.com