

# STATE OF TREASURY FRAUD

*A Disconnect Between Perception, Response, & Reality*

## PERCEPTION

84%

### Heightened Threat Perceived

84% of corporates believe the threat of cyber fraud and payment fraud has increased over the past year.



26%\*

### Continued Security Investments

26% of corporates are planning to spend more or significantly more on treasury security compared to last year.

\* Data excludes "Unsure" responses.

20x

### Increased Corporate Confidence

20x more corporates believe they are in a better position to deal with fraud this year compared to last year.

## RESPONSE

29%

### Piecemeal Approach to Security

Only 29% of corporates have developed a formal treasury fraud and controls framework, while over 2/3<sup>ds</sup> of banks have done so.

-10%

### Reconciliation Capabilities Decline

Over the past three years, there has been a 10% DECREASE in the number of firms that reconcile 90%+ of their accounts daily.



3x

### Fraud Management Responsibilities Unassigned

Nearly 3x more banks than corporates have formally assigned fraud monitoring roles.

## REALITY



300%

### Growth in Ransomware

The frequency of ransomware attacks grew by over 300% between 2017 and 2018.

40%

### Increase in Fraud Experience

There has been a 40% year-over-year rise in fraud activity perpetrated against the treasury environment since 2016.

10-30%

### Criminal Success Rates

Today's criminal enjoys a 10%-30% success rate for techniques ranging from check forgery and ransomware to PCard and BEC fraud.

[DOWNLOAD NOW](#)