Payment Fraud Prevention for Banks: Budgets, Spending and Losses

Published 2 February 2024 - ID G00806082 - 13 min read

By Analyst(s): Pete Redshaw

Initiatives: Banking Industry Technology Insights

A survey of FS leaders shows how much of their budgets they allocate to fraud prevention for payments, the proportion that is spent externally on software and services, and the relative losses they incur. CIOs can compare their own spending to the overall survey results.

Overview

Key Findings

- There is a wide spread of spending on fraud prevention. This illustrates that banks have very different starting points: many have old, homegrown systems with no AI at all that need to be replaced, while others have multiple modern but siloed systems that need to be integrated and consolidated.
- The spending on payments fraud prevention has been exacerbated by the continuing expansion of real-time payments around the world, meaning that suspicious transactions have to be identified within much less than one second and then acted upon.
- External spending by banks on fraud prevention is focused on challenges such as a holistic approach to fraud and security; the impact of new payment rails, such as real-time payments (RTP), on fraud types; and the application of machine learning (ML) technology to fraud detection.

Recommendations

- If RTP are soon to be initiated in your region or locality (or have just been launched), check if you are ready to deal with new kinds of attacks and at the high speed that is necessary. Are your fraud prevention systems also near real time and can they initiate the necessary actions (e.g., putting a suspected fraudulent transaction on hold, near-real-time reporting in dashboards with period-by-period comparisons)?
- Monitor on a regular basis (monthly or quarterly) the proportion of all fraud losses that are due to payments losses. Check if this proportion is roughly static or declining/increasing over time, and how it correlates with spending in this area.
- Determine if you have sufficient in-house talent for maintaining the machine learning (ML) models for fraud, for case investigations and for migrating to the cloud. If you do not, investigate which of your vendors can help close this talent gap.
- Put in place a strategy for closer integration of your suite of fraud and security solutions and how you can enable a “big picture” view for patterns, spikes and clusters of attacks across all those systems. Consider whether a best-of-breed approach is best for this closer integration or whether you need to adopt something closer to a one-stop shop approach and choose a primary vendor.

Data Insights

Banking payments fraud prevention is a major concern for banks, yet it accounts for a relatively small portion of total IT spending. A recent survey of FS leaders investigated how they invest in fraud prevention software and services and, in particular, these four data points:

- Considering their overall IT budget, what is the percentage that is allocated for **general fraud prevention?**
- Considering their spending on general fraud prevention, what is the percentage that is allocated specifically for **payments fraud prevention**?
- Considering their spending on payments fraud prevention, what are the percentages that are allocated for **external spending** on (a) services and (b) software?
- Considering the total losses due to fraud that their organizations experience each year, what percentage of those **losses** are due to payments fraud specifically?

Certain drivers and trends for spending on fraud prevention are already clear:

- Spending on fraud prevention will increase. Our 2024 CIO survey for banks shows that:
  - 78% of CIOs intend to spend more on cyber/information security.
  - Cybersecurity and risk management is the No. 2 focus area for CIOs in the next 12 months.
  - Faud/risk management is the No. 2 use case for AI/GenAI.
- Just as AI/GenAI is helping banks to combat fraud, it also helps criminals to perpetrate increasingly sophisticated fraud attacks. This creates a vicious circle of competing forces that ratchets up spending.
- There will be increased focus on how fraud is prevented (and dealt with when it happens) as regulations become more rigorous, liability shifts toward the bank, customers must be protected and the bank's reputation must be preserved to maintain trust.

Hence, there is a need for CIOs and heads of fraud at banks to understand — and compare — how a particular bank's approach to spending on fraud prevention corresponds to, or diverges from, the averages shown here. However, banks vary considerably in their level of preparedness and efficiency when it comes to fraud prevention, so the level of investment needed to achieve an acceptable outcome at a specific bank will also vary accordingly. This is a small and varied sample, so it is only an illustrative snapshot of the current situation at 64 financial services institutions (FSIs), and it does not dictate a "right" level of spending.

Online Fraud Prevention Spending

Fraud prevention needs increasingly sophisticated and expensive technology to be effective; yet, it still accounts for a relatively small portion of the total IT spend at banks. The Gartner Financial Services Research Panel Survey, October 2023, queried bank executives and leaders. [1] A question posed was: "Considering your overall IT budget, what is the percentage that is allocated for general (online) fraud prevention?"

Fraud prevention (which here excludes fraud perpetrated by internal employees) is defined as IT spending to:

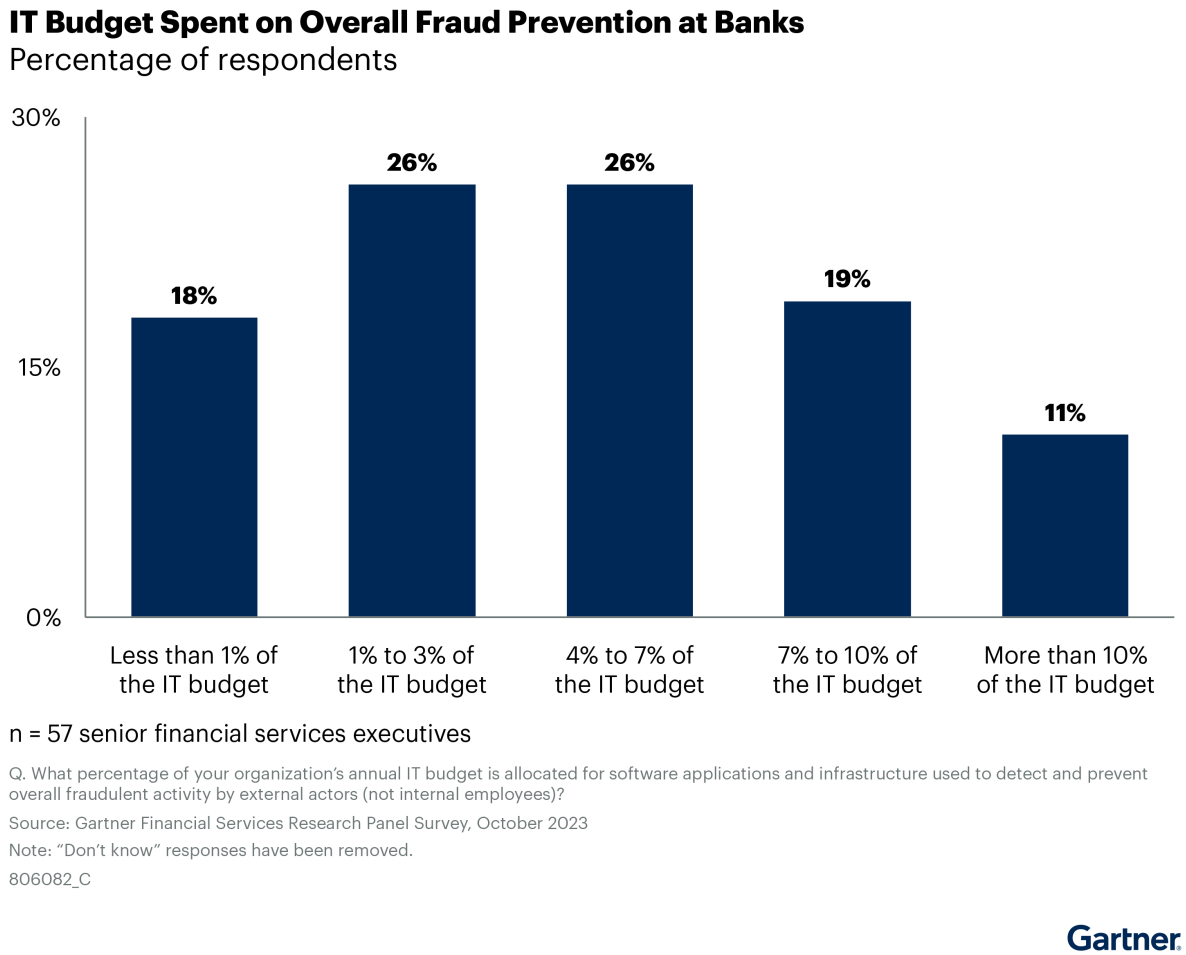
- Detect scams (such as authorized push payments, money mules, false chargebacks and phishing)

- Protect against account takeover and malware
- Comply with anti-money laundering, sanctions, screening and KYC requirements
- Implement capabilities for identity verification, device ID, location intel, bot mitigation and behavioral biometrics

As Figure 1 shows, 89% of the banks responding to this survey stated that they allocate 10% or less of their total IT budget to fraud prevention, and nearly half spend less than 3%. That may not sound like much, but bear in mind that banking outspends most other industries. Banks have some of the world's biggest IT budgets, so even 1% of the total can still be many millions of dollars. Even so, a striking aspect of the data in Figure 1 is the spread of spending within that bracket. This illustrates that banks have very different starting points. Our interactions with them tell us that some have old, homegrown systems with no AI at all that need to be replaced, while others have multiple modern but siloed systems that need to be integrated and consolidated. Fraud prevention is a top priority, and fraud attacks are increasingly sophisticated, so spending on prevention will inevitably increase over time.

A very topical concern here is the impact that generative AI will have as it is adopted by fraudsters. For example, it can be used to generate much more convincing text for fake emails without the telltale grammatical and syntactical errors of old. It's an unfortunate fact of life that new technologies may benefit the criminals as much as they aid banks and their customers; hence, the unceasing race for banks to master each new innovation before their enemies do.

Figure 1: IT Budget Spent on Overall Fraud Prevention at Banks



Spending on Payments Fraud Prevention

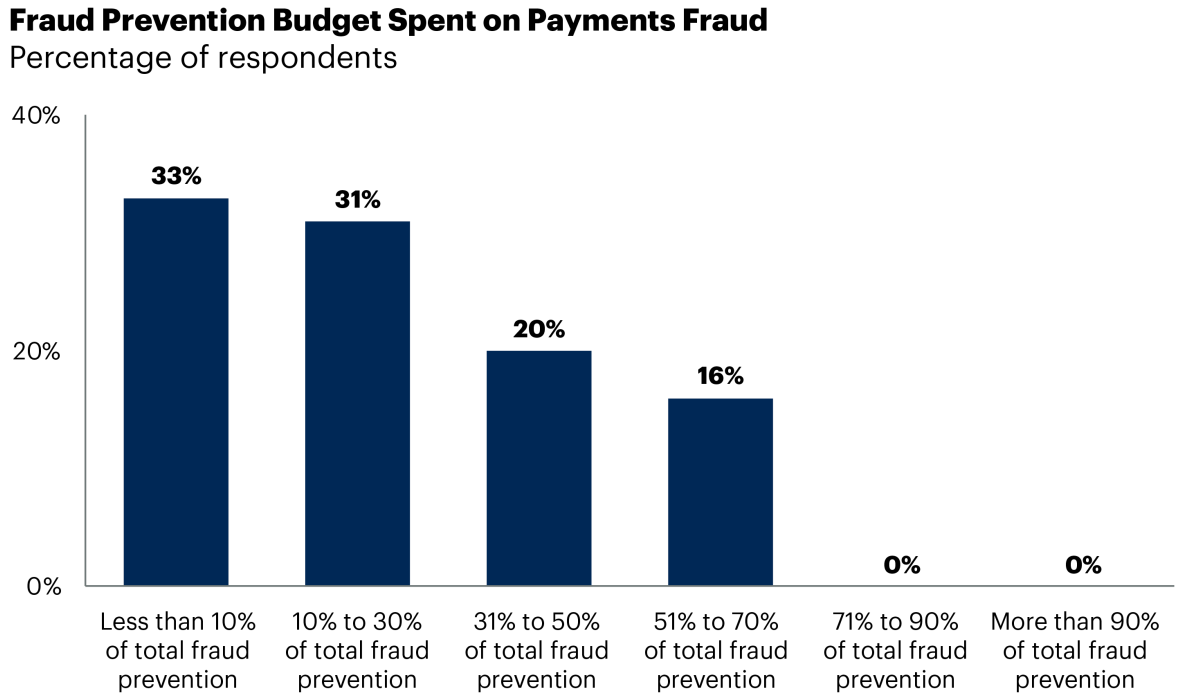
Focusing specifically on payments fraud prevention, our survey question was: "Considering what your organization spends annually on overall fraud prevention, what is the average percentage of that total which is spent specifically on preventing payments fraud (i.e., the percentage spent on transaction monitoring for payments events)?"

As Figure 2 shows, 36% of the banks responding to this survey stated that they allocate 30% or more of their overall fraud budget on payments fraud prevention. Therefore, payments are of considerable importance within the overall gamut of fraud prevention. This has been exacerbated by the continuing expansion of real-time payments around the world, meaning that suspicious transactions have to be identified within much less than one second and then acted upon.

Payment fraud here is regarded as any online fraud that involves falsely creating or diverting payments. Payment fraud includes, but is not limited to:

- Creating bogus customer records and bank accounts so that false payments can be generated.
- Stealing another person's payment information — or tricking them into sharing it — to make false or illegal transactions.
- Intercepting and altering payee details and amounts on checks and payable orders, then attempting to cash them.

Figure 2: Fraud Prevention Budget Spent on Payments Fraud



n = 49 senior financial services executives

Q. Considering what your organization spends annually on overall fraud prevention, what is the average percentage of that total which is spent specifically on preventing payments fraud (i.e., the percentage spent on transaction monitoring for payments events)?

Source: Gartner Financial Services Research Panel Survey, October 2023

Note: "Don't know" responses have been removed.

806082_C

Gartner

External Spending for Payments Fraud Solutions

External spending typically accounts for a significant portion of banks' payment fraud prevention. This spending falls into two main categories. Figure 3 shows that banks allocate, according to the mean average:

- 29% of their total payments fraud prevention spending on external services.

- 38% of their total payments fraud prevention spending on external software.

Banks look externally for help with three main challenges in this domain:

- A holistic approach to fraud and security.
- The impact of new payment rails, such as real-time payments (RTP), on fraud types.
- The application of machine learning (ML) technology to fraud detection.

A Holistic Approach

The chief advantage of a holistic approach is the opportunity to enhance the integration (most often using data orchestration tools) between the many security and fraud solutions at a bank. Breaking down the silos between fragmented solutions helps to eliminate the gaps that are exploited by fraudsters (see Emerging Tech: Security — Cyber-Fraud Fusion Is the Future of Online Fraud Detection). External spending can help by utilizing vendors that have preintegrated these solutions and offer something closer to a "one-stop shop" portfolio of solutions and services.

New Payment Rails Like RTP

RTP is a boon to consumers, but it also raises the risk of some types of fraud like authorized push payments (APP). Banks lose the luxury of an overnight batch settlement in which to catch and rectify attempted fraud. Hence, external help is needed with the technology to detect and act on suspected fraud at subsecond speed while improving (or at least maintaining) the detection and accuracy rates of their algorithms. Vendors can also help to mitigate the impact by connecting (where available) their platforms to national initiatives such as Confirmation of Payee (aka Account Validation). These help check the validity of the beneficiary account, which may be pretending to be something that it is not, at another bank.

Machine Learning Technology

Fraud attacks now mutate quickly, and the systems to prevent them must evolve quickly, too. This means daily updates to the features of the ML models that are used and rapid retraining of the models. Vendors have already started to shift from the old 100% reliance on supervised training (using static, historical datasets with the fraudulent transactions labeled) to unsupervised training (using live feeds of new data in a near-real-time feedback loop). Modern systems should prompt data scientists at the bank with suggestions about which features and rules to modify/add/retire. The process remains semiautomatic because banks need to test the changes before putting them into production in the revised ML model or the business rule engine that typically exists in parallel. Once assured that the changes are an improvement in terms of detention rate and accuracy, then the degree of manual effort needed to make them live needs to be limited. Systems should provide the equivalent of a "fire-and-forget" button that can deploy the changes with minimal human intervention.

Figure 3: External Spending for Payments Fraud Solutions

n = 48-49 senior financial services executives

Q. Of the money that your organization spends on payments fraud prevention, what percentage of that is spent externally on (i) software and (ii) services?

Source: Gartner Financial Services Research Panel Survey, October 2023

Note: "Don't know" responses have been removed.

Note: Percentages may not add up to 100% due to rounding.

806082_C

Gartner

Losses Due to Payments Fraud

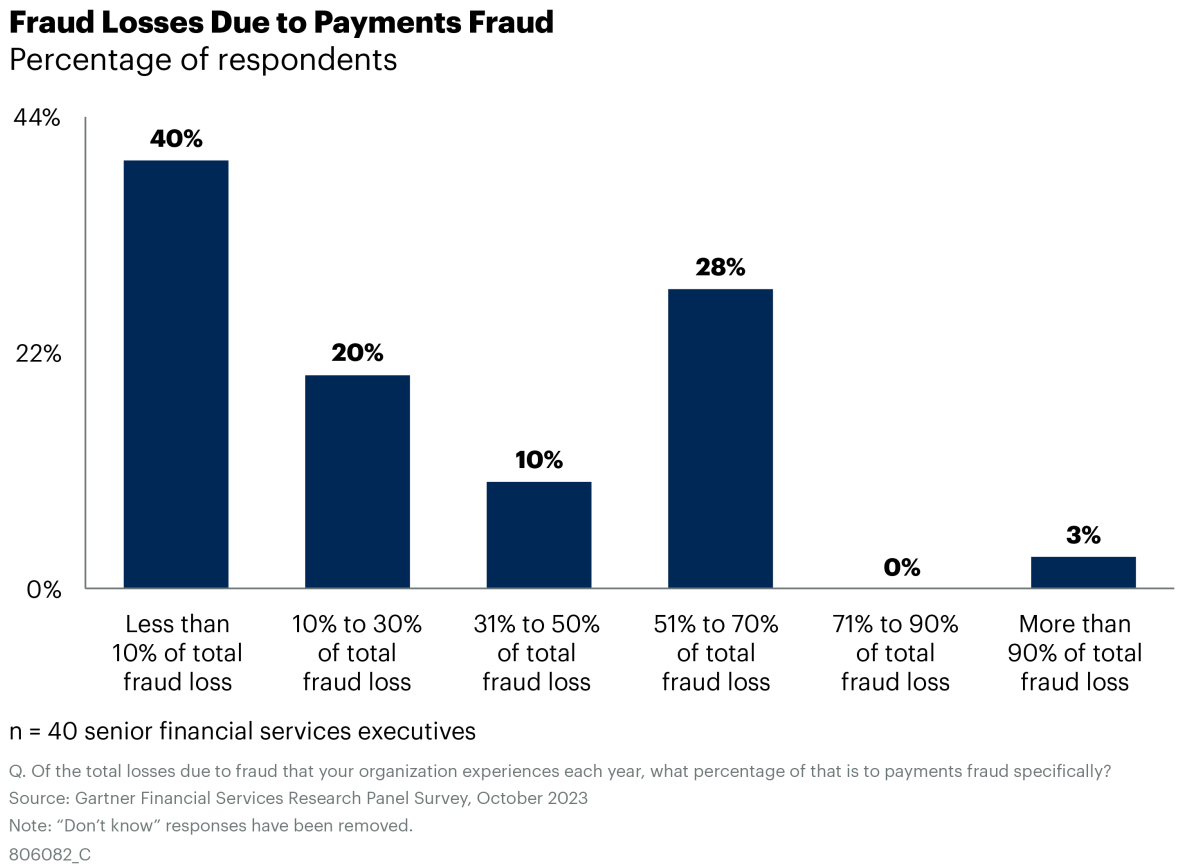
Focusing on the losses incurred by banks that are specific to payments fraud prevention, the question posed to bank executives and leaders was: "Of the total losses due to fraud that your organization experiences each year, what percentage of that is to payments fraud specifically?"

Figure 4 shows that 60% of the banks responding to this survey stated that 30% or less of all fraud losses were due to payments fraud. But there is some polarization here. There is another group (31% of the responding banks) where payments fraud is more than 50% of all fraud losses. In short, it tends to be relatively low for most banks, but there is a significant minority where it is relatively high (and the remaining 10% of banks are somewhere in the middle of this valley). The emergence of new payment rails and new technologies such as GenAI may lead to spending on payments fraud prevention being a larger proportion of all fraud prevention; however, only time — and more data — will tell if that hypothesis is true.

This polarization is interesting, and there is a variety of possible explanations such as:

- Most obviously, payments is a much bigger line of business at some banks than at others.
- Also, some banks are much better at payments fraud prevention than others because they have invested in the latest technology and have deployed effective processes around those solutions.
- Payments fraud may be more prevalent in some countries than others (possibly those where RTP is relatively new and there has been a spike in new kinds of fraud attack).
- The variation in how different banks allocate fraud to different categories (e.g., payment fraud vs. identity fraud vs. account takeover) may be hidden in the results.
- The size of a bank may be a nonlinear factor in determining the ratio of fraud losses to all losses (e.g., small banks may not benefit from the economies of scale that large banks have as a result of their vast volumes of payments).

Figure 4: Fraud Losses Due to Payments Fraud



CIOs and heads of fraud can measure their own spending in these areas and then compare it to the business outcome at their bank. Based on the outcome of that exercise, there are some near-term and long-term actions to consider as follows.

Near-Term Actions

- If RTP is soon to be initiated in your region or locality (or has just been launched), check if you are ready to deal with new kinds of attacks (such as APP) and at the high speed that is necessary. Are your fraud prevention systems also near real time and can they initiate the necessary actions (e.g., putting a suspected fraudulent transaction on hold, near real time reporting in dashboards with period-by-period comparisons)?
- Investigate how GenAI can be used to augment your fraud prevention systems in the areas of content discovery (e.g., unusual customer behavior) and simulation of attacks (i.e., stress testing).

- Monitor on a regular basis (monthly or quarterly) the proportion of all fraud losses that are due to payments losses. Check if this proportion is roughly static or declining/increasing over time, and how it correlates with spending in this area.
- Check if you have sufficient in-house talent for maintaining the ML models for fraud, for case investigations and for migrating to the cloud. If you do not, investigate which of your vendors can help close this talent gap.

Longer-Term Actions

- Put in place a strategy for closer integration of your suite of fraud and security solutions and how you can enable a "big picture" view for patterns, spikes and clusters of attacks across all those systems. Consider whether a best-of-breed approach is best for this closer integration or whether you need to adopt something closer to a one-stop shop approach and choose a primary vendor.
- Investigate the opportunities for collaboration with other banks regarding fraud prevention and how your vendors can facilitate such consortia and sharing.
- In addition to current skills gaps, anticipate future requirements. For each identified gap, consider whether it can be closed through training existing staff or if new hiring is necessary.

Evidence

[1] **Gartner Financial Services Research Panel Survey, October 2023.** This survey was conducted online from 19 October through 02 November 2023. In total, 64 senior executives at financial services organizations participated. All 64 participants were members of Gartner's Financial Services Research Panel, a Gartner-managed panel.

Disclaimer: Results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.

Recommended by the Author

Some documents may not be available as part of your current Gartner subscription.

Buyer's Guide for Fraud Detection Technology in Banking

Tool: RFP Questionnaire Template for Fraud Detection in Banking

Emerging Tech: Security — Cyber-Fraud Fusion Is the Future of Online Fraud Detection