# HSBC Ignored Years of Warnings From Fraud Managers Who Wanted BioCatch as Scammers Stole Millions

*The Bank's Own Fraud Experts Wanted To Implement BioCatch and Threatmetrix, but they could not get the budget!*


HSBC failed to act on repeated warnings from its own fraud experts after scammers had stolen millions from hundreds of Australian customers.

Internal documents that were filed in court by the *Australian Securities and Investments Commission* shows the bank's fraud team repeatedly warned that "losses will continue to mount" without proper security measures, but the bank failed to implement on their recommendations and didn't want to invest the money on the tools.

The ASIC is now suing HSBC Australia for "widespread and systemic" failures that allowed criminals to impersonate bank staff and drain their customer's accounts.

## "No Real-Time Interception": Years of Warnings From The Fraud Team That No One Wanted To Hear

According to court filings, the warnings were all there in black and white – and there were lots of presentations about it from the fraud team.

In March 2021, HSBC fraud staff gave an internal presentation that the bank had "no real-time interception or payment-holding to clarify suspicious transaction content with customers ."

This feature, if they had it, would have allowed the bank to pause suspicious transactions before money left customer accounts.  Maybe HSBC was being a bit cheap because the solution would have costed $380,000 to implement, according to the documents.

The warnings grew more urgent over time as the fraud managers saw it happening more and more each month.

"Currently, HSBC do not have the capability to stop an online transfer of funds from one bank account to another," stated another presentation to the bank's fraud steering committee in October 2022.

## The Head Of Fraud Presented On Impersonation Scams

The court documents even show how the Head of Fraud at the bank presented on the topic of impersonation scams and their impacts.

In July 2023, **Matthew Hannan, HSBC Australia's head of fraud management**, was making a "special" presentation about an "HSBC impersonation scam" that had already victimized 50 customers.

Two months later, another internal presentation warned that "current limitations

on desktop banking monitoring and real-time interception are impacting our ability to disrupt and prevent these attacks."

## How the Scam Worked: Fake Texts and Stolen Life Savings

The scams which occurred between 2023 and 2024, were the very same scams the hit the UK and the US.

Scammers contacted HSBC customers via text messages or calls that appeared to come directly from the bank.  They claimed to be bank fraud staff attempting to stop suspicious transactions on their accounts.

"The irony of these cases is that fraudsters were claiming to do what the bank itself could not – detect and stop suspicious transactions in their tracks," according to court documents.

Once the customers called the phone number back, they were tricked into sharing security passcodes and personal information, believing they were helping reverse fraudulent charges.

Some customers lost their entire life savings in the scheme. Court documents revealed that one group of fraudsters linked to the scam used local HSBC accounts to move stolen money to beneficiaries in Pakistan.

## The Fraud Managers Wanted To Buy ThreatMetrix and BioCatch But The Steering Committee Turned Them Down

ASIC alleges that HSBC Australia didn't implement adequate real-time fraud payment monitoring capabilities until May 2024, years after the first warnings and at the tail end of the scam operation.

The bank also failed to deploy two key fraud tools BioCatch, and ThreatMetrix until June 2024.  These were the fraud systems that the bank had failed to invest in years earlier when the impersonation scams began.

In January 2022, minutes from a fraud steering committee meeting there notes that "losses resulting from these scam cases and determinations would likely have been

avoided with BioCatch/ThreatMetrix implementation for transactional monitoring."

But the fraud team didn't give up. In fact they tried again. In December 2023, as customer losses increased even more, another internal presentation warned that until these systems were implemented, the fraud team "cannot disrupt scams, and losses will continue to mount."

## The Bank Could Have Stopped $50 Million In Scams But They Didn't Want To Spend The $380,000 On Fraud Tools

The financial impact on customers was very large. Customers of HSBC lost $18 million on impersonation scams in the 2023 financial year alone, according to court documents. And to make matters worse, during the first nine months of 2024 those scam losses spiked to $24 million.

ASIC Deputy Chair Sarah Court said in a statement that HSBC Australia's failings had devastating consequences for customers. "We allege that from at least January 2023, HSBC Australia was aware of the risks of unauthorized transactions occurring and that there were gaps in their fraud controls," she said. "This resulted in some customers getting scammed out of $90,000 or more."

*The lesson learned here? Listen to your fraud managers!*