COMPLIANCE & RISK

Fraud-driven de-risking: A crucial strategy for enhancing banks' financial security

Ingo Steinhaeuser Senior Risk and Fraud Specialist / Thomson Reuters

15 Mar 2024 · 5 minute read

Financial institutions may be financially responsible for some of the behavior of their customers; to that end, they tend to end some client relationships to limit their risk and exposure, but as fraud increases, it's even more important to surveil account activity and limit risks

The concept of de-risking is nothing new. Banks at times will discontinue a business relationship if the profile of a client appears too risky or if indicators pointing to fraudulent activities are uncovered.

The termination of some client relationships might appear unjust, such as the reported case of a restaurant owner making rounded cash deposits, or a client deemed too risky due to familial connections in Nigeria. In most cases, however, termination actions are justifiable, and banks tend to **terminate banking relationships** for the right reasons.

And there are ample reasons. Data from suspicious activity reports (SARs) have shown a steep increase in fraud schemes targeting various segments of banking customers. Indeed, the large number of fraudulent payment transactions underscores the need to protect banking customers through a systematic approach using a variety of means and tools. When bank payments can be carried out instantly with a few commands on an app, thus reducing the speed of the transaction, it limits the possibility for corrections, since the funds might be already transferred once the fraud has been detected.

Defining banks' obligations

Banks' obligations are mainly defined and regulated under the Electronic Fund Transfer Act, in which banks are required to reimburse victims when unauthorized payments occur. For example, if a customer reports an unauthorized electronic fund transfer within two business days, the customer's liability is limited to $50. If that window stretches to 60 days, the customer's liability increases to $500. After 60 days, a bank can legally hold customers liable for any fraudulent transactions related to their accounts. Reporting the fraud when it occurred is therefore of crucial importance.

Data from suspicious activity reports (SARs) have shown a steep increase in fraud schemes targeting various segments of banking customers.

The case of Zelle, a payment network owned by seven of the largest US banks, may be the best example of the changing approach to reimbursing customers. Facing regulatory pressure, Zelle's operator, Early Warning Services, has initiated reimbursements for victims of imposter scams, expanding such repayments beyond the legal obligations. This is clearly a new precedent for the banking industry's responsibility towards its customers, and more than 2,000 financial firms have begun **reversing transfers that their customers made** to imposters of government agencies, banks, and other fraudulent service providers.

That voluntary reimbursements by financial firms might be a new normal, is further supported by a recent lawsuit of the New York State Attorney General's office against Citibank for not safeguarding its customers enough against electronic fraud and for failing to compensate those who were affected.

The apparent lack of oversight has resulted in the loss of millions of dollars for Citi's customers. And according to the lawsuit, Citibank's insufficient security measures made it simple for fraudsters to infiltrate customers' accounts and illicitly withdraw funds through unauthorized wire transfers. It would be highly unusual that one of the largest financial institutions has insufficient control mechanisms in place.

If Citi loses this lawsuit, it will set a precedent that the burden of responsibility moves from the consumer to the bank with severe consequences for the industry.

Financial institutions have a variety of tools at their disposal... [and] these techniques can provide further intelligence into the activities and the origin of a fraudulent customer and spot problems before they turn into larger losses.

A re-evaluation of risk management strategies and stricter transaction controls will likely be the result of such a verdict. In fact, it may change fundamentally how banks are monitoring client activities and increasing controls. Terminations of banking relationships with customers that represent an uncomfortable level of risk based on a multitude of factors — such as the inability to follow recommended security protocols like multi-factor authentication, the level of password strength, or lack of receiver verification — will need to be taken into consideration. It will be an understandable move and could be justified to shareholders if the correlation between profitability and unbanked individuals proves to be positive.

How to stop the diverse nature of fraud

The types of non-loan fraud schemes that are increasing show replicable patterns of activity and require a different approach to prevent. In fact, growing fraud schemes like account takeovers, synthetic ID fraud, or new account fraud require a multitude of tools and techniques for prevention and detection.

To prevent these, financial institutions have a variety of tools at their disposal, not just with data analytics and artificial intelligence, but also, by using biometric capabilities that allow for the identification of a customer during or before a transaction, behavioral capabilities in combination with device & network recognition, and location-based insight. All of these techniques can provide further intelligence into the activities and the origin of a fraudulent customer and spot problems before they turn into larger losses.

As fraudsters exploit human vulnerabilities by leveraging cognitive biases and emotional triggers and using tactics such as authority, urgency, and affinity to manipulate unsuspecting customers, technology cannot safeguard clients alone. Education and training of both banking staff and end-use customers are equally important.

As the Zelle case has shown, banks are reimbursing customers beyond their legal obligations. In cases where a customer is acting in gross negligence — which is often the case in romance, online shopping, and investment scams — educating customers is critical as banks will not reimburse losses occurred in such cases.

The financial industry is characterized by a shared responsibility model, and to maintain that de-risking is an essential component of safeguarding. Beyond technological capabilities, building trust and verifying customers through personal contact might be another solution to an emerging problem especially as the financial sector continues to grow and evolve.

BUSINESS FRAUD COMPLIANCE & RISK CORPORATES FINANCIAL INSTITUTIONS GOVERNMENT REPUTATIONAL RISK RISK FRAUD & COMPLIANCE RISK MANAGEMENT