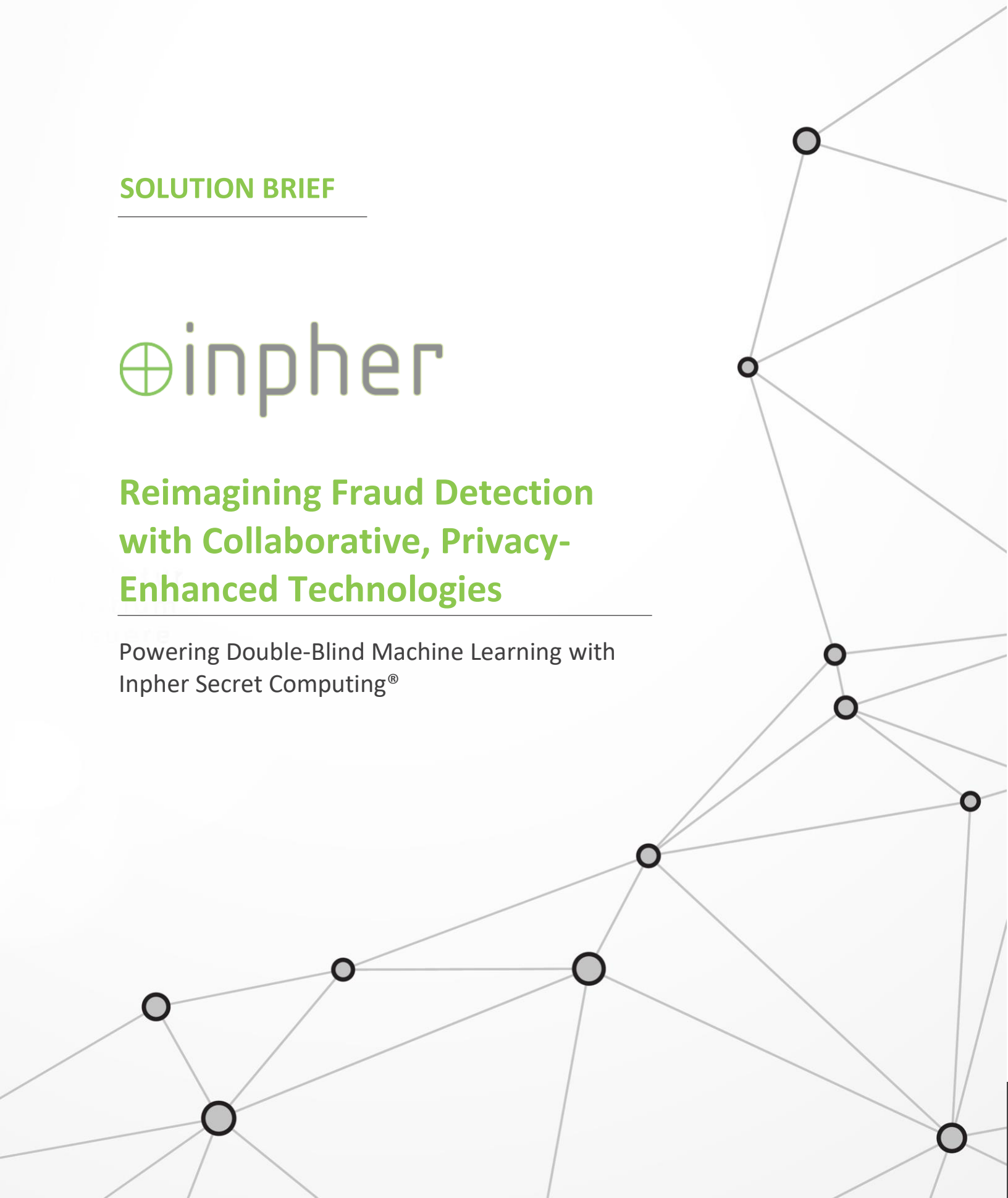
SOLUTION BRIEF

inpher

Reimagining Fraud Detection with Collaborative, Privacy-Enhanced Technologies

Powering Double-Blind Machine Learning with Inpher Secret Computing®



Reimagining Fraud Detection with Collaborative, Privacy-Enhanced Technologies

Powering Double-Blind Machine Learning Through Inpher Secret Computing®

Financial crimes cost businesses billions of dollars each year, not just in the form of direct losses but also from regulatory fines and damages to their brand. Companies are increasingly relying on ML algorithms to identify fraudulent transactions. Yet, the lack of data access due to regulatory compliance leads to less accurate fraud detection models, thereby requiring manual interventions. Given the millions of transactions in a month, financial organizations face significant transaction delays, bad customer experience, and, eventually, lost revenue. Inpher's Secret Computing technology helps them build models by fostering collaboration across various departments or even with other institutions without sharing their data. This allows financial institutions to securely, privately, and compliantly take down financial criminal networks.

"Data Limited' ML Often the Only Option

Existing fraud detection ML algorithms typically assign a fraud indicator (0 or 1) or a probability score to each processed transaction. Any transaction that acquires enough indicators, or scores above a certain threshold, are paused and sorted for manual review. Unfortunately, due to the high volume of transactions processed and the

Accurate, Precise Fraud Detection

Find patterns of fraud by unlocking the hidden insights from data silos

Improve Data Science Productivity

Empower data science teams by delivering privacy-preserving data all from their notebook

Foster Collaboration

Create and manage privacy enhanced collaboration at scale

Exceed Compliance Needs

Leverage power of data while complying with global privacy and data regulators such as GDPR and CCPA

fear of losing clients' money, rule thresholds are often set low. Millions of transactions are processed in a day, and thousands of resulting transactions are flagged for manual review, each taking 3-5-days of further scrutiny. This forces financial organizations to expend significant resources to execute a manual process. Data science teams could address these challenges, improving ML algorithm precision vastly if they could access more *features*. These features are often scattered across various departments (credit card, mortgage, wire transfer, etc.) or geographical silos due to privacy and compliance restrictions.

Future of Fraud Detection with Inpher's Secret Computing

Inpher's Secret Computing empowers financial organizations and banks to modernize their privacy-preserving AI and analytics experience. With Secret Computing, organizations can leverage hidden insights from third-party data by collaborating with other parts of their company or even other organizations securely to improve their fraud models. The cryptographic nature of Secret Computing prevents the external transfer and exposure of transaction of data while allowing participating data sources to secretly share insights that improve model accuracy. This collaborative network of financial data silos is integral to monitoring and combating advanced financial crimes and fraudulent activities quickly and accurately. We call this a "Secret Computing Network."

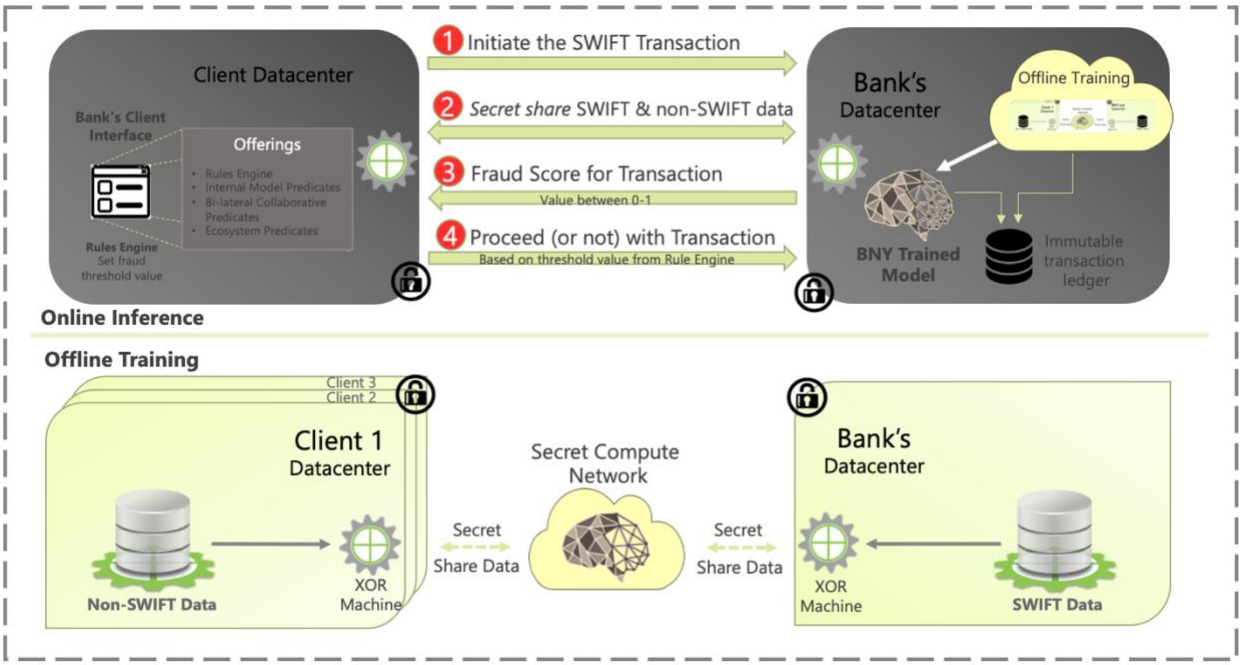
Secret Computing in Real World

"Double-blind Machine Learning for fraud detection at BNY has been colloquially known as *Sinking Pirates*. Now that cloud computing has provided the elastic scale required to use Data Science as our next strategic tool for fighting fraud, the next big hurdle is assembling large-enough, current-enough training data sets. Investing in obtaining more training data is a lot more effective than work to improve models. Yet, we will continue to do both because the cost of financial fraud robs us all of the resources better used elsewhere while funding criminal activities that threaten civilization. The 'bad guys' have all the same technologies we do. But the one thing they cannot obtain is the scale of training data we can through collaborative sharing, such as through what Inpher offers with Secret Computing. Training models to prevent and counter fraud using data that we cannot or would prefer not to share otherwise offers an excellent advantage for beating the criminals and keeping them beaten."

Hays W. "Skip" McCormick
Data Science and Architecture Fellow

BNY MELLON

A Secret Computing Network is designed to be the most accurate option for financial organizations on a simple premise: More (Good) Data equals Better Fraud Detection. The outcome is that by catching more fraudulent transactions, they can offer better services to their clients, earning more of their business. Secret Computing, powered by the XOR product, seamlessly integrates with existing ML workflow, making it easier for data science teams to build privacy-preserving models.



During the offline training phase, Inpher's XOR Machine is installed across all the privacy zones. Intra-organization privacy zones could be credit card transaction logs, mortgage payment logs, credit score logs, or online transaction logs. Privacy zones across financial organizations could be the SWIFT provider and the client bank using the service. By training a model with multi-dimensional features across these privacy zones, the fraud detection precision will be significantly increased and highly accurate given the large data sets that the model is training on while never exposing raw data between the intermediaries, thus guaranteeing privacy.

Why Are Regulators Excited About Secret Computing?

Regulators are increasingly interested in exploring how financial institutions can securely share insights without exposing underlying data to fight financial crimes. Organizations such as the Financial Conduct Authority (FCA) hold the Global AML and Financial Crime TechSprint every year, looking for innovative ways to solve these challenges. In one such TechSprint, the purpose was to determine how privacy-enhancing technologies (PETs) can effectively combat financial crime, detect fraudulent activities, and prevent money laundering within the financial service industry. Inpher Secret Computing won the People's Choice Award for the best solution to solve fraud detection.