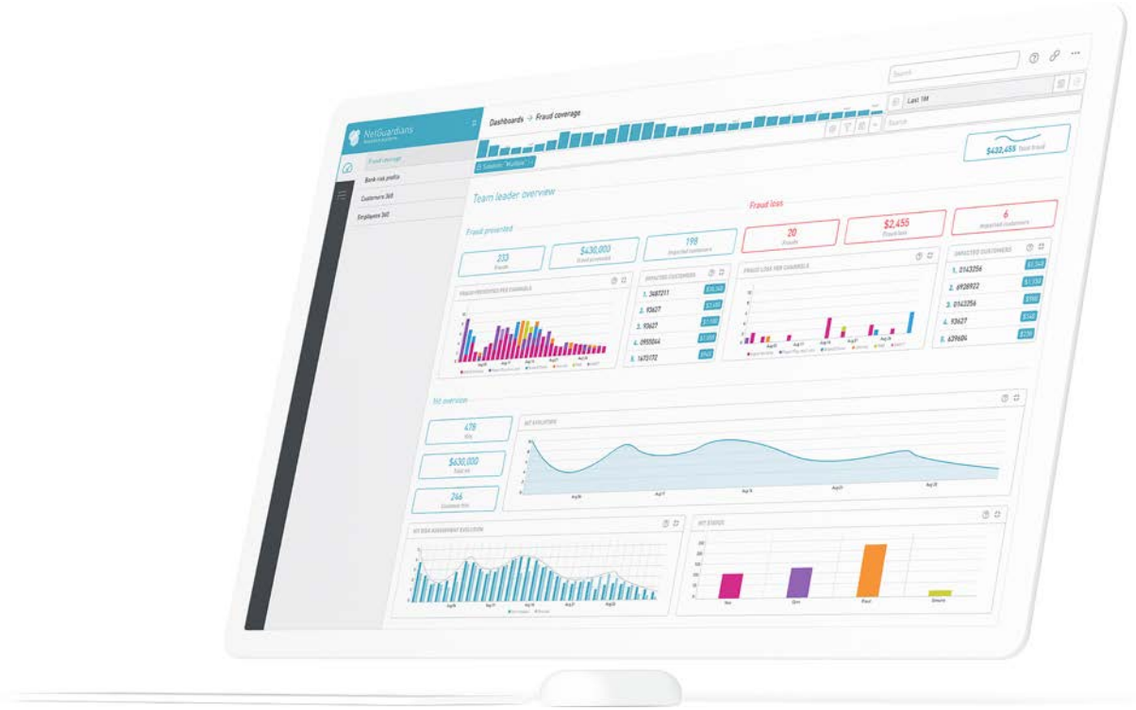
FINASTRA NetGuardians

Factsheet – Fusion Fraud Prevention Service

Fraud prevention for Finastra's service bureau customers

Real-time, AI-powered fraud prevention for payment messages



The fraud problem

Today's bank robbers prefer cybercrime. Among the biggest and most successful heists in recent years was the theft of $81 million from the Central Bank of Bangladesh in 2016 using the SWIFT network and local infrastructure.

Since then, there have been plenty more hacks over banking networks, helping lift the expected cost of cybercrime globally to $10.5 trillion by 2025*.

In response, SWIFT created the SWIFT Customer Security Program (CSP). At the heart is the Customer Security Controls Framework (CSCF), detailing what must be implemented by all SWIFT members.

A key set of controls relates to the prevention and detection of fraud. To help combat fraudulent activities, between July and December 2022, all financial institutions will need to attest their compliance with the CSCF v2022. A key change from 2021 is that control 2.9 (Transaction Business Controls) becomes mandatory. This control demands firms "implement transaction detection, prevention, and validation controls to ensure outbound transaction activity within the expected bounds of normal business."

As SWIFT payments are increasingly moving – and even settling – in near real-time, after-the-fact fraud detection is no longer sufficient. Banks need to monitor for fraud in real-time, too. The challenge is to do this accurately and effectively, especially when cyber fraudsters frequently change attack vectors to avoid detection.

* Cyber Security Ventures, Cyber Crime Report 2020

Behavioral monitoring of SWIFT and other payment messages without time-consuming rule configuration

Tailored for Finastra's SWIFT Service Bureau customers and integrated with Fusion Total Messaging, the NetGuardians solution for SWIFT messages enables financial institutions to identify and stop fraudulent SWIFT messages in real-time, before they are released to the SWIFT network.

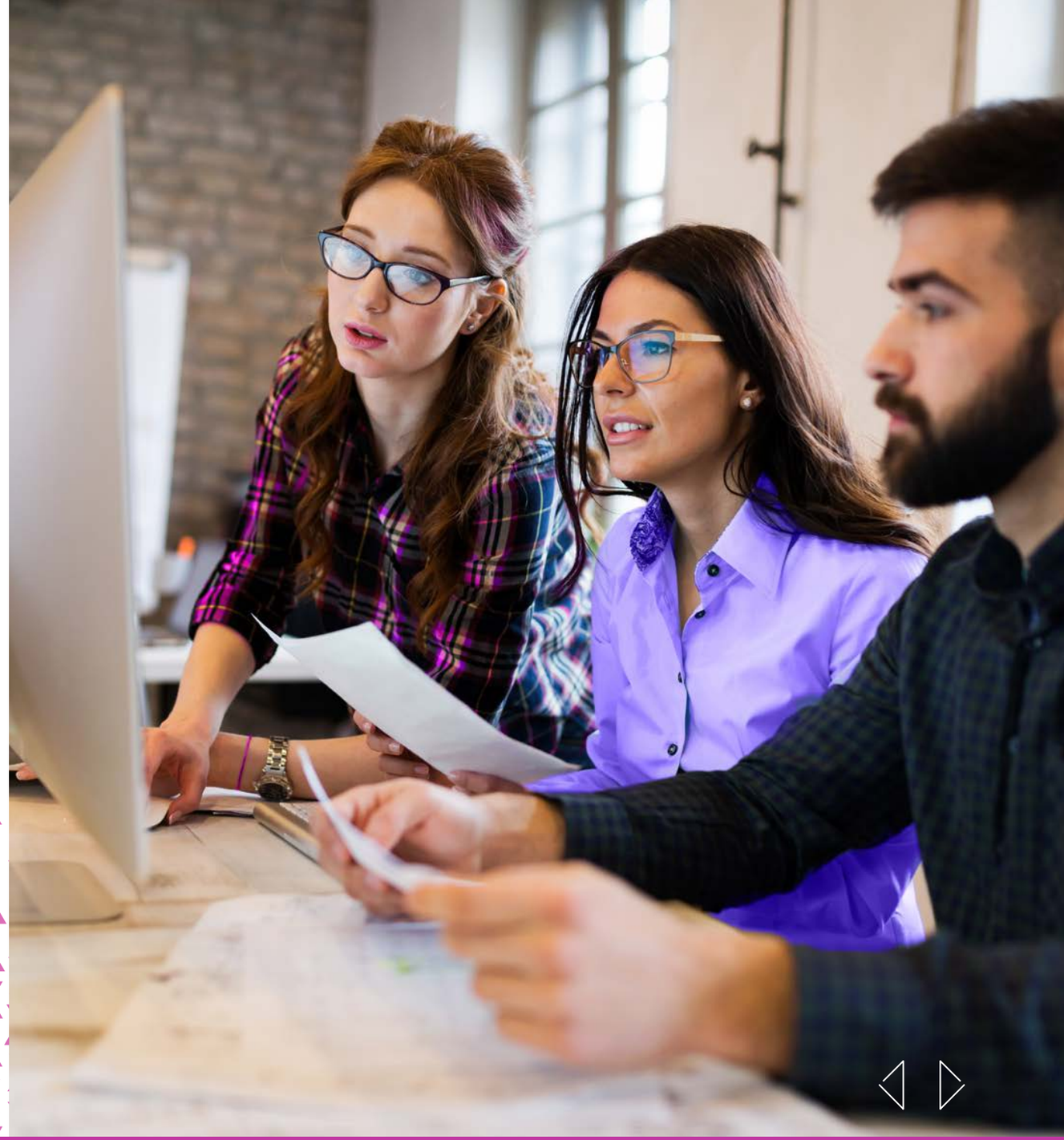
Any suspicious messages are held for investigation. This SaaS solution is hosted securely by Finastra, remote from your local infrastructure.

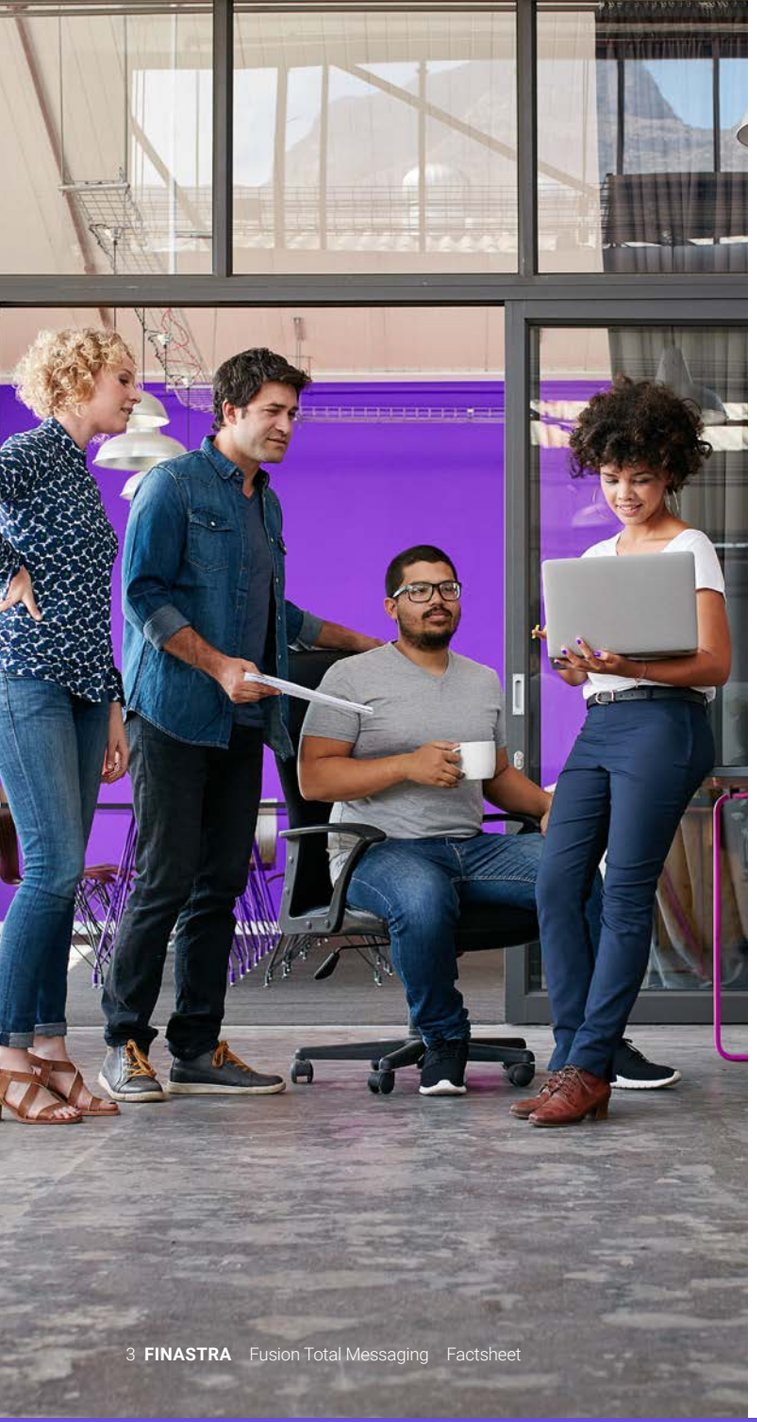
Powered by NetGuardians' machine learning and artificial intelligence technologies, the solution "reads" each customer's SWIFT messages – including MT 101, MT 103, MT 202 and MT 202COV – and learns how to accurately stop fraudulent payments.

It reduces operational costs and also saves time because it learns automatically, so there's no need to configure new rules in the system. The NetGuardians solution can also accommodate additional payment messages (e.g., SIC, euroSIC, etc.).

The solution's behavioral risk models detect anomalous activity resulting from a combination of attributes including:

- New beneficiary (for the customer and/or the bank)
- Unusual amount (e.g., out of the norm for the customer account)
- Unusual destination (for the customer and/or the bank)
- Unusual timeframes (e.g., days, times, frequency)





A holistic approach to fraud prevention

Real-time fraud prevention with flexible transaction workflows

Abnormal or suspicious SWIFT messages are detected in real-time. Flexible transaction workflows allow for blocking, alerting, releasing and reporting.

Low false positives

The system's analytic approach is much more accurate than relying on rules. It leads to lower operational costs and an improved customer experience, with fewer valid payments incorrectly blocked. A recent case study* highlighted that a bank switching to NetGuardians reduced false positives by 83%, while at the same time increasing their fraud detection rate.

SWIFT CSP compliance

Pre-configured AI risk models continuously monitor MT 101, MT 103, MT 202 and MT 202COV messages to identify anomalous and possibly fraudulent activities.

Community

Financial institutions opting to use NetGuardians' fraud prevention solution for SWIFT become part of a growing community of fraud prevention experts, and they are provided a trusted forum for sharing their experiences of fraud.

Detection of new fraud types

By nature, fraudulent messages are always anomalies for the instructing party. NetGuardians' solution continuously learns about the payment behavior of the instructing party and the bank as a whole. It uses machine learning to detect anomalies, identifying new fraud scenarios without the need to pre-configure targeted rules in the system.

Augmented intelligence

The NetGuardians solution uses "augmented intelligence," which combines human intelligence with machine learning and AI technology to effectively flag anomalous SWIFT messages. A Case Manager provides contextual information about each alert so users can clearly understand why the transaction is suspicious. Workflows, forensic tools and dashboards are intuitive and easy-to-use, enabling rapid investigation of suspect transactions and efficient case handling and record-keeping.

*NetGuardians case study

Benefits

Effective fraud detection

AI-powered SaaS solution that's highly effective at detecting known and unknown fraud scenarios for various payment messages, using anomaly detection and supervised learning approaches.

Rapid implementation

Because it is part of Finastra's existing financial messaging system, the solution is already integrated with Fusion Total Messaging, so it can be activated quickly.

Saves time

Hosted by Finastra's Service Bureau, which frees up time for your IT staff for other important tasks.

For more information, please contact your Finastra account manager or contact us.

About Finastra

Finastra is building an open platform that accelerates collaboration and innovation in financial services, creating better experiences for people, businesses and communities. Supported by the broadest and deepest portfolio of financial services software, Finastra delivers this vitally important technology to financial institutions of all sizes across the globe, including 90 of the world's top 100 banks. Our open architecture approach brings together a number of partners and innovators. Together we are leading the way in which applications are written, deployed and consumed in financial services to evolve with the changing needs of customers. Learn more at **finastra.com**

Finastra and the Finastra 'ribbon' mark are trademarks of the Finastra group companies.
© 2021 Finastra. All rights reserved.

Corporate Headquarters
4 Kingdom Street
Paddington
London W2 6BD
United Kingdom
T: +44 20 3320 5000

ID-6729 / 1121