Titre:19 years of exquisite SWIFT experience: Will 2020 be the Expertus Technologies consecration year with a new certification? - Connect and find out Why?

Sous-Titre: Swift recognizes Expertus Technologies expertise by, once again, renewing its certification

Intro

Expertus Technologies, has successfully finalised the certification process for its Shared Infrastructure Programme (SIP) for 2020. SIP is a well-known certification at Expertus since it has been over 19 years today, that we meet every year with undeniable success..You must know that Expertus has been a SWIFT Partner since 2002 and certified Service Bureau since 2007 and is playing a major role in the North America market being a top SWIFT solution provider , with a solid reputation to provide global payment capabilities and infrastructure management services alongside its unique innovative solutions.

In fact, to be certified SWIFT Service Bureau means that Expertus Technologies fulfils the highest security and availability needs and standards. Audited onsite by Swift auditor, the experience carries out a demanding global review including all technical aspects, infrastructure design and security controls. Operating the Service bureau is limited only to certified Swift experts, ensuring every single detail meets the Swift requirements and best practices. Expertus Swift team carries more than 70 years of experience with Swift products.

Let us look at this high-end certification definition and target:

- The SIP defines eligibility criteria, roles, and responsibilities, as well as legal, financial, and operational requirements that Service bureau must always meet.
- Our last Swift onsite inspection was carried out in 2019.

Expertus helps its clients as well in their Customer Security Program (CSP) Self Attestation

The SWIFT CSP aims to ensure the security and integrity of the systems that connect to the SWIFT network. By securing and protecting their local environments, the SWIFT CSP works with the members of the financial services industry to prevent future cyber attacks.

What is the benefit for our customers? What does it mean in concrete terms, for our Ceo, Jacques Leblanc?

"It's a true honor for us to have these Swift certifications, there is a true recognition for the processing of financial messages through the SWIFT network with transparency, high lead integrity, validity and skills in secure environment for our customer by improving our each time our skill expertise.

With the SWIFT Team, we regularly review and adapt the SIP to reflect market and technical developments and the evolving threat landscape.

It is an accumulation of years and years of experience, it is a very critical and demanding field and is an essential service for banks, financial institutions, and corporates. We are proud to be able to offer this level of security and reliability to our customers and to contribute with so much passion and rigor to energize our Canadian financial ecosystem internationally.

We, at Expertus Technologies are so excited to renew our 19 year partnership with Swift to provide the best financially secure system to our customers! "

About Expertus Technologies

Expertus Technologies is a Montreal-based Fintech specializing in innovative payments and treasury solutions. As a pioneer in

Cloud solutions for financial services, Expertus helps accelerates payments modernization and transformation

through its various offerings in the modern Expertus Payments Platform. Expertus provides outsourced services

and products that the institutions leverage for international wires, ISO migration, mass payments, fraud control

and connectivity to various platforms including SWIFT. For more information please contact **sales@expertus.ca**

Visit our website

https://www.expertus.ca/

SWIFT Customer Security Program

Time to get ready

Key dates

- End of Q1 2017: CSP standards finalized
- Start of Q2 2017: First annual self-attestation against 16 mandatory controls
- 1 January 2018: SWIFT starts enforcement, inspections and disclosures on non-compliance against the mandatory controls; customers can expand their disclosures to cover 11 advisory controls

Immediate next steps

- Establish cross-functional team to oversee CSP implementation, including risk, compliance, technology, legal and operations
- Conduct readiness assessment against mandatory and advisory controls
- Assess how attestation requirements align with existing Service Organization Control (SOC) reporting
- Determine how SWIFT CSP effort should align with broader payments cybersecurity initiatives
- Review past audit, risk, IT/information security findings/assessments to identify critical gaps to be addressed as part of CSP implementation
- Evaluate where manual interventions are required for processing to determine potential technological solutions

Over the past few years, financial services policymakers and regulators have realized that it is now a matter of when, not if, the industry will suffer a major system-wide disruption, one that aims to destroy. Well-publicized attacks in the last 12 months have made this feel probable, not just plausible. Not surprisingly, the regulatory focus has increasingly shifted to systemic cyber risks and the weakest links across the system, not just within regulated institutions. New or proposed regulatory standards are being issued more frequently.

Within this shift, there is an even more enhanced focus on the security of the Society for Worldwide Interbank Financial Telecommunications (SWIFT). SWIFT Chief Executive Officer Gottfried Leibbrandt said of the attacks on the Bangladesh Bank, "[They] will prove to be a watershed event for the banking industry; there will be a before and an after Bangladesh."[1] Enhancing SWIFT security is critical for global financial markets. After all, it processes 6.1 billion transactions a year, of which a significant minority (around one-fifth) are processed with manual intervention, and it has more than 11,000 customers.

SWIFT's most prominent new initiative is its Customer Security Program (CSP), which takes effect this year. Starting in the second quarter of 2017, SWIFT's customers will have to attest to complying with 16 mandatory controls. In January 2018, SWIFT will start sharing information on non-compliance with customers' regulators and counterparties and enforcing compliance by randomly selecting customers who will be required to provide additional information from their internal or external auditors. SWIFT customers will have the option to adopt 11 more advisory (i.e., voluntary) controls and to go beyond self-attestation to self-inspection by internal audit, or third-party inspections.

The CSP covers a range of issues that are now becoming commonplace in new and more demanding – and now increasingly mandatory – requirements, notably the need for:

- Strong access, privilege, password and database controls, and multi-factor authentication
- Detailed knowledge of, and controls over, data flows linkages to business processes, and dependencies on external critical vendors

[1] Martin Arnold, "Swift outlines fightback against cyber theft," 23 May, 2016, *Financial Times*

Fraud Detection on SWIFT Messages without the need to configure rules

Bank heists used to involve guns, dynamite and a bag for the swag. Not anymore. Today, thieves are getting away with millions using just zeros and ones – they are hacking their way in. Among the biggest and most sophisticated was the successful $81m heist at the Central Bank of Bangladesh in 2016 using the SWIFT network and local infrastructure. Since then there have been plenty more hacks over the banking networks, helping lift the expected cost of cyber crime globally to $6tn by 2021*.

In response SWIFT has drawn up the SWIFT Customer Security Program (CSP), a mandatory set of security controls that must be implemented by all SWIFT members. In order to be compliant, financial institutions must prevent and detect fraud in commercial relationships and continuously share information and collaborate to better prepare for future cyber attacks.

SWIFT CSP mandatory controls related to the first line of defense cannot cope with the high-profile and high-cost cyber heists. Advanced transaction monitoring related to SWIFT messages is needed to help financial institutions meet SWIFT CSP requirements.

NetGuardians

Recognized as Gartner Cool Vendor and Chartis RiskTech 100 Vendor, NetGuardians is helping financial institutions worldwide to fight financial crime.

Transaction monitoring and no-effort detection of anomalous activity on SWIFT messages

NetGuardians' Fraud Detection for SWIFT messages enables financial institutions to identify and stop fraudulent transaction messages before released to the SWIFT network, in real time. Powered by NetGuardians' machine learning and augmented intelligence technology, the solution automatically learn from SWIFT MT 101, 103 and 202COV messages and captures unusual message parameters to ultimately suspend and alert on fraudulent transactions.

Examples of at-risk situations addressed by Fraud Detection for SWIFT messages:

Anomalous activity related to:

- → Time-frame (e.g. unusual time of day, unusual frequency)
- → Unusual payment instructions
- → Unusual payment value (e.g. amount bigger than usual)
- → Unusual or new relationships (e.g. new beneficiary payment to a new country unused by FI)

* Cyber Security Ventures, Cyber Crime Report 2016