



**NATIONAL
SETTLEMENT
DEPOSITORY**
MOSCOW EXCHANGE GROUP

WFC Board Meeting
Prague, 11 May 2017

FINTECH AND CYBER RESILIENCE

FINTECH OVERVIEW IN NSD

DEVELOP FINTECH ECOSYSTEM

- SWIFT Innotribe Startup Challenge, Russia, Jul 2017 as a partner
- RISE Financial Technologies partnership to launch DLT-based Commercial papers
- Open API for fintech startups to bring the institutional bond market to the masses

COLLABORATE TO BE LEADERS

- DLT Working group of 6 CSDs for use case development
- Product requirements for Proxy voting completed in April 2017
- ISSA support for DLT WG initiative
- Joint effort with SWIFT for ISO 20022 alignment & DLT standardization
- New members considering to join in 2017

LEVERAGE NEW TECHNOLOGIES

- DLT-based Proxy voting platform developed & planned for production in 2017
- Add-on to Hyperledger blockchain platform to support confidentiality of client accounts in shared ledger environment

PROVIDE TECHNOLOGICAL SERVICES FOR THE MARKET

- eVoting platform for GM / the first voting with the #1 Russian bank this season
- Connectivity: SWIFT Service Bureau and "Transit" service for every Russian financial market participant



NOBODY IS SAFE

CYBER ATTACKS are now not geek hacker activity, it's an organized crime, they know your business and it's vulnerabilities well

- If you never performed **PENETRATION TESTS** carried out by external specialists and never simulated cyber attack then your investments into cyber security could be a futile
- If you switch from your main site to **DISASTER RECOVERY SITE** less than once a year (or even never) then you most probably don't have a disaster recovery site and disaster recovery plan
- The more **DIGITAL SERVICES** you introduce the more spots for possible attacks you create
- The more you **OUTSOURCE** the more cyber security risk you create



CYBER SECURITY: CSD SPECIFIC



*AGMs, dividend payments, etc.



WHAT NSD DOES



Participates and contributes in Central Bank of Russia's activities: working groups, mailing lists, seminars



Participates in SWIFT 'Customer Security Programme'



Revises most critical points: e.g. additional and more strict certification of SWIFT connectivity



Performs penetration tests for critical systems



Performs regular switching from main site to disaster-recovery site



Provides board supervision for cyber security unit's activities

CASE STUDY: SWIFT CSP PROGRAMME

Designed within several months as a response to a several notorious cyber attacks, including attacks on FMIs

Internal SWIFT taskforce is under very senior management supervision; Engages all SWIFT customers globally

Engages all SWIFT customers globally

National and local FMIs are key participants and competence centers

Counts on network effect

Community is the main object of protection

You can get more details on the topic:
<https://www.swift.com/myswift/customer-security-programme-csp>



KEY TAKEAWAYS AND IMMEDIATE ACTIONS

- 1** **REVISE CYBER SECURITY** supervision and governance system within your company
- 2** Review your most critical **3RD PARTY PROVIDERS**
- 3** Be sure you **EDUCATE YOUR EMPLOYEES** in terms of awareness, behavioral patterns (e.g. you found a flash drive in your office, what would you do)
- 4** Make everyone aware, cyber security is a process which **INVOLVES ALL COMPANY**
- 5** **JOIN YOUR EFFORTS**: participate in relevant to communities' activities (e.g. "Customer Security Programme" by SWIFT, or your regulator's actions)
- 6** Create **CROSS-FUNCTIONAL TASKFORCE** and set cyber security related KPIs for top-management
- 7** Make sure cyber security unit's activities are visible, understood and gain enough **SUPPORT WITHIN YOUR COMPANY**

THANK YOU!



**NATIONAL
SETTLEMENT
DEPOSITORY**
MOSCOW EXCHANGE GROUP

DISCLAIMER

- This presentation has been prepared and issued by NSD (the “**Company**”). Unless otherwise stated, the Company is the source for all data contained in this document. Such data is provided as at the date of this document and is subject to change without notice
- This document does not constitute or form part of, and should not be construed as, an offer or invitation for the sale or subscription of, or a solicitation of any offer to buy or subscribe for, any securities, nor shall it or any part of it or the fact of its distribution form the basis of, or be relied on in connection with, any offer, contract, commitment or investment decision relating thereto, nor does it constitute a recommendation regarding the securities of the Company
- The information in this document has not been independently verified. No representation or warranty, express or implied, is made as to, and no reliance should be placed on, the fairness, accuracy or completeness of the information or opinions contained herein. None of the Company, or any of its subsidiaries or affiliates or any of such person's directors, officers or employees, advisers or other representatives, accepts any liability whatsoever (whether in negligence or otherwise) arising, directly or indirectly, from the use of this document or otherwise arising in connection therewith
- This presentation includes forward-looking statements. All statements other than statements of historical fact included in this presentation, including, without limitation, those regarding our financial position, business strategy, management plans and objectives for future operations are forward-looking statements. These forward-looking statements involve known and unknown risks, uncertainties and other factors, which may cause our actual results, performance, achievements or industry results to be materially different from those expressed or implied by these forward-looking statements. These forward-looking statements are based on numerous assumptions regarding our present and future business strategies and the environment in which we expect to operate in the future. Important factors that could cause our actual results, performance, achievements or industry results to differ materially from those in the forward-looking statements include, among other factors:
 - Perception of market services offered by the Company and its subsidiaries
 - Volatility (a) of the Russian economy and the securities market and (b) sectors with a high level of competition that the Company and its subsidiaries operate
 - Changes in (a) domestic and international legislation and tax regulation and (b) state policies related to financial markets and securities markets
 - Competition increase from new players on the Russian market
 - The ability to keep pace with rapid changes in science and technology environment, including the ability to use advanced features that are popular with the Company's and its subsidiaries' customers
 - The ability to maintain continuity of the process of introduction of new competitive products and services, while keeping the competitiveness
 - The ability to attract new customers on the domestic market and in foreign jurisdictions
 - The ability to increase the offer of products in foreign jurisdictions
- Forward-looking statements speak only as of the date of this presentation and we expressly disclaim any obligation or undertaking to release any update of, or revisions to, any forward-looking statements in this presentation as a result of any change in our expectations or any change in events, conditions or circumstances on which these forward-looking statements are based

