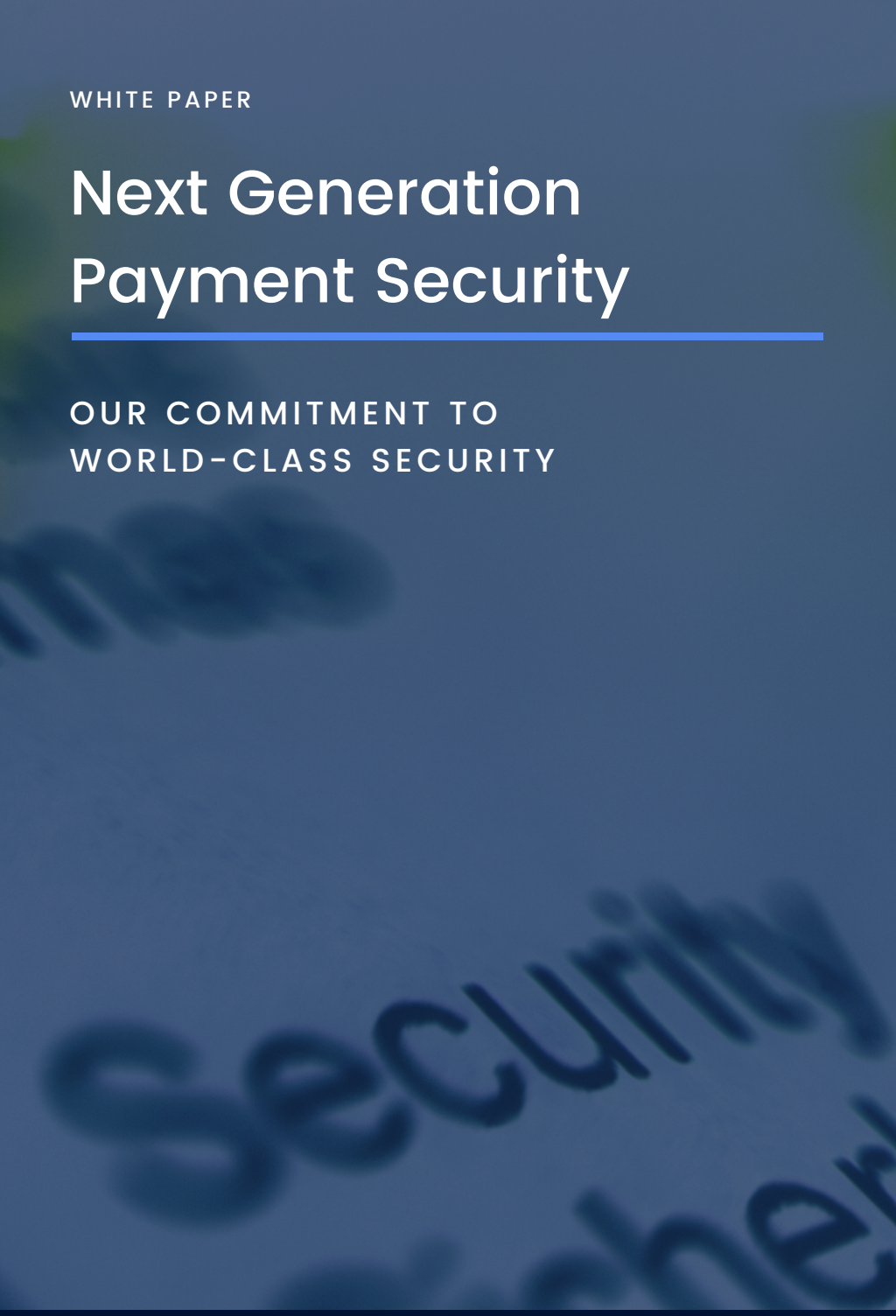
WHITE PAPER

Next Generation Payment Security

OUR COMMITMENT TO WORLD-CLASS SECURITY



plooto

Index

Introduction

Payment security has received a lot of attention lately. Many companies have become victims of financial and sensitive data breaches. Lack of IT spending, complex architecture, technology fragmentation as well as antiquated and legacy systems have left many companies vulnerable to cyberattacks.

This is precisely why Plooto's number one priority is security. Our cloud based solution delivers the most secure and most up to date security standards on par with the top financial institutions. Plooto consistently meets or exceeds the stringent security requirements of even the most security conscious organizations including Fortune 500 companies, the world's largest financial institutions, and other global companies.

Plooto has been designed from ground up with security and compliance at the forefront. The following white paper identifies the security guidelines and processes Plooto has put in place to ensure continuous delivery of a secure platform that surpasses customer expectations.

Payment Network

All Canadian payments processed with Plooto are settled through our partnership with members of Payments Canada. Plooto's payment technology is built on top of the existing banking infrastructure which is developed and maintained by Payments Canada.

Payments Canada is a non-profit organization that operates clearing and settlement systems in Canada and is responsible for the following:

- Operate and maintain national systems for the clearing and settlement of payments and other arrangements for making or exchanging of payments.
- Facilitates the interaction of the CPA's systems with others involved in the exchange, clearing and settlement of payments.
- Facilitates the development of new payment methods and technologies.

As a trusted Payments Canada partner, Plooto can process payments to any Bank or Credit Union in Canada and US.

Plooto underwent verifications and approvals within the following key areas to meet the requirements of Payments Canada:

FULL COMPANY BACKGROUND AND RISK ANALYSIS

Full financial and background auditing of our business processes and financials was preformed by our banking partners.

SECURE DATA TRANSFER/COMMUNICATION

Our system was validated for both incoming and outgoing data exchange using secure channels. Secure File Transfer Protocol is designed by Internet Engineering Task Force (IETF) and is powering data exchange for most major financial institutions.

SYSTEM INTEGRATION COMPATIBILITY

Continuous tests are performed to ensure payment instructions are reflecting user actions during the payment cycle. We also run daily tests to ensure that the system is responsive for both recipient and sender's bank communications.

In conjunction with Payments Canada requirements, Plooto has implemented additional in-house security measures such as policy based fund clearing, bank account ownership verification as well as personal identity verification.

Cloud Platform Infrastructure

All of Plooto's infrastructure elements are hosted by Microsoft Azure through its Infrastructure as a Service (IaaS) business unit.

Microsoft, with its unique experience and scale, delivers cloud services to many of the world's leading enterprises and government agencies. Today, the Microsoft cloud infrastructure supports over 1 billion customers across their enterprise and consumer services in 140 countries and supports 10 languages and 24 currencies.

PHYSICAL SECURITY

Azure provides geographically distributed data centres that comply with industry standards (such as ISO 27001) for physical security and availability. Facilities are designed to run 24x7x365 and employ various measures from power failure to network outages. Centralized monitoring is administered by operations personnel.

ANTIVIRUS AND ANTI-MALWARE

Virus and anti-malware software scans all production and testing deployments using industry certified tools that ensure clean and stable environment. Routinely scheduled scans ensure that in the event of a breach systems will remain threat free.

NETWORK AND DATA ISOLATION

Logical isolation and segregated environments ensure confidential data remains inaccessible to unauthorized parties.

ENCRYPTING DATA AT REST AND IN TRANSIT

All traffic within the Plooto application is encrypted using built-in cryptographic technology with TDS (TabularData Stream) and SSL (secure sockets layer) when stored in Azure's data centres. This ensures that data is never exposed to unauthorized third parties.

Plooto Platform

Plooto's secure platform encompasses our network and data security, platform security and workflow security.

NETWORK AND DATA SECURITY

End-to-End Encryption

All communication between users and Plooto is encrypted using the latest Secure Hash Algorithm 2 (SHA2) SSL Certificates. This standard is being utilized by top financial institutions and ensures no data is intercepted by unauthorized parties.

Encrypted Internal Communication

All internal system data remains encrypted (using SSL) to prevent loss.Data EncryptionAll customers' sensitive data is encrypted using AES 256 bit (Advanced Encryption Standard). This standard has been widely adopted by Canadian and U.S. governments and is utilized worldwide.

Data at Rest Encryption

Additional levels of encryption are applied to ensure data is encrypted while residing on physical hardware.

ISO CERTIFIED

Extending to both physical and digital security, Plooto is certified under the ISO 27001 standard. Regular external audits are enforced to maintain this certification and continuous updates are made to security policies accordingly.

ACCESS CONTROLS FOR YOUR DATA

Plooto does not store data unless it's needed to provide you excellent service or to comply with the law. Plooto will never store details like your social security number or bank login credentials. Plooto employees will never ask for your password through any form of communication, and do not have access to that information. Further, only a handful of specially trained employees have access to the data you share to complete your company verification (KYC) process.

PLATFORM SECURITY

Staff Background Checks

All Plooto employees, vendors, and contractors go through a thorough vetting process including background checks conducted externally as well by Plooto's compliance team.

Customer Data Access Monitoring

Access to the data by personnel is monitored, auditable, enforced by roles and is secured through multi-factor authentication.

PROACTIVE SECURITY POLICY

Plooto enforces password policy with enough entropy to be next to impossible to break. Passwords are not stored in plain text but rather hashed using PBKDF2 (Password-Based Key Derivation Function 2). Failed authentication attempts are tracked. Additional attempts will trigger security verification and could cause the account to be locked in severe cases.

SECURE TWO-FACTOR AUTHENTICATION

Plooto offers secure two-factor authentication login for all users. This means that you will have additional protection against account threats such as login information theft and phishing attempts.

INSURANCE POLICY

Plooto holds a comprehensive insurance policy to protect both Plooto and our valued customers for additional peace of mind. Our insurance policy is held by one of the largest insurance providers in the world. Plooto's insurance coverage includes cyber crime protection, financial crime and theft protection, and professional liability insurance to name a few.

Bank Account Validation

Financial institutions use sophisticated mathematical algorithms to generate and authenticate account information keyed into their system. Transaction instructions submitted by Plooto to a bank are validated using these algorithms.

Modulus Check Digit Routines use checksum formulas in order to validate account numbers. TheModulus 10 routine is used by Plooto, financial institutions and government agencies as a method of distinguishing valid numbers from mistyped or otherwise incorrect numbers. These algorithms were specifically designed to protect against accidental errors when entering bank account information electronically.

Modulus routines involve multiplying some or all of the digits in the branch and/or account number by fixed numbers (the weighting factors). There is a specific weighting factor for each digit used in the verification process. The result of each multiplication is summed and the total divided by a specific modulus number.In the event banking information is reported as invalid, the Plooto system flags the transaction and electronically notifies our system administrators.

Conclusion

Plooto's security strategy allows us to ensure the confidentiality and privacy of our customers' information, and enables us to deliver 99.99% up-time and availability of our system. We meet or exceed international security standards and deliver exceptional financial and data security. Our continuous security enhancements, employee training, and close partnerships with leading technology and payment providers demonstrates our commitment to world-class security.

Do you have any questions or want to request further details about Plooto's security policies or the manner in which we treat your personal information?

Contact Plooto's Information Security Representative at:

compliance@plooto.com