MONETA values the work done by security researchers in improving the security of our products and services. The safety of our internet banking and continuity of our online services are our top priorities. Despite our continuous effort, vulnerabilities in our systems can still be present. We actively encourage anyone who believes they have discovered a vulnerability in our systems to act immediately to help us improve and strengthen the safety of our systems by sharing it with us.

Responsible Disclosure Guidelines

We will investigate legitimate reports and make every effort to quickly correct any vulnerability. To encourage responsible reporting, we **will not take legal action** against you nor ask law enforcement to investigate you provided you comply with the following Responsible Disclosure Guidelines:

- Provide details of the vulnerability, including information needed to reproduce and validate the vulnerability and a Proof of Concept (POC).
- Make a good faith effort to avoid property or non-material damage, privacy violations, destruction of data, and interruption or degradation of our services.
- Do not modify or access data that does not belong to you.
- Do not attempt to penetrate the system any further than required for the purpose of your investigation. Should you have successfully penetrated the system, do not share this gained access with any others.
- Do not utilise social engineering in order to gain access to our IT systems.
- Do not utilise any brute-force techniques (e.g. repeatedly entering passwords) in order to gain access to the system.
- You will not disclose the vulnerabilities found to any third party without the prior consent of MONETA.

How to report a vulnerability

Please report any product or service-related issues directly to vulnerability@moneta.cz, using our PGP key to encrypt reports containing sensitive information. Please write your report in a clear and concise way, include the product, where you found the issue and as many details as possible to help us identify the exact area of the issue. Offering a solution is highly encouraged but not required.

What to report

In general, we are interested in receiving reports on vulnerabilities that:

- Enable disclosure of non-public client information.
- Enable a user to modify data that is not their own.
- Could lead to compromise or leakage of data and directly affect the confidentiality or integrity of user data or which affects user privacy.

Specifically, we are interested in any of the following vulnerabilities:

- Cross-site request forgery (CSRF/XSRF)
- Cross-site scripting (XSS)
- Authentication bypass / unauthorised data access
- Encryption vulnerabilities
- Remote code execution
- Injection vulnerabilities
- Privilege escalation

This document is not a Public promise or Promise of indemnity within the meaning of the Civil Code. However, we do not exclude the possibility of a decision to reward a vulnerability report that will benefit MONETA, depending on the circumstances of the case.

Ve společnostech MONETA si ceníme práce výzkumníků v oblasti bezpečnosti při zlepšování bezpečnosti našich produktů a služeb. Zejména bezpečnost internetového bankovnictví a kontinuita našich online služeb je naší nejvyšší prioritou. Navzdory našemu neustálému úsilí se mohou v našich systémech vyskytnout případné chyby. Aktivně podporujeme každého, kdo věří, že objevil zranitelnost v našich systémech, aby ji okamžitě nahlásil a pomohl nám zlepšit a posílit bezpečnost našich systémů.

Pokyny pro zodpovědné nahlášení zranitelností

Všechny relevantní zprávy prověříme a vynaložíme maximální úsilí k opravě případných zranitelností. Abychom podpořili zodpovědné nahlášení, **nebudeme proti vám podnikat právní kroky**, ani nebudeme iniciovat zahájení vyšetřování ze strany orgánů činných v trestním řízení, pokud dodržíte následující pokyny pro zodpovědné nahlášení zranitelností:

- Poskytnete nám podrobnosti o zranitelnosti, včetně informací potřebných pro reprodukci a ověření zranitelnosti (tzv. Proof of Concept).
- Vynaložíte maximální úsilí, aby nedošlo ke způsobení majetkové škody či nemajetkové újmy, porušení soukromí, zničení dat a přerušení nebo zhoršení našich služeb.
- Neupravíte ani nepřistoupíte k datům, které vám nepatří.
- Nebudete se pokoušet proniknout dále do systému, než je nutné pro účely vašeho výzkumu. Pokud jste úspěšně pronikli do systému, nebudete sdílet tento přístup s dalšími lidmi.
- Nebudete používat sociální inženýrství k získání přístupu do našich systémů.
- Nebudete používat techniky hrubé síly (tzv. brute-force) k získání přístupu do našich systémů (např. opakované zadávání hesel).
- Nezveřejníte ani nesdělíte třetím osobám nalezené zranitelnosti bez předchozího souhlasu společností MONETA.

Jak nahlásit zranitelnost

Jakékoli problémy týkající se bezpečnosti produktů nebo služeb, prosím nahlaste přímo na vulnerability@moneta.cz, pomocí našeho PGP klíče zašifrujte citlivé informace. Svou zprávu formulujte prosím jasně a stručně, uveďte příslušný produkt, ve kterém jste objevili zranitelnost a co nejvíce detailů, které nám umožní identifikaci konkrétní oblasti, ve které se zranitelnost nachází. Případné návrhy na řešení problému nejsou nezbytné, ale uvítáme je.

Co nahlásit

Budeme rádi, pokud nám nahlásíte zranitelnosti které:

- Umožňují zveřejnění klientských údajů.
- Umožňují uživatelům modifikovat data, která nejsou jejich.
- Mohou vést ke kompromitaci nebo úniku dat a přímo ovlivnit důvěrnost nebo integritu uživatelských dat nebo ovlivnit soukromí uživatelů.

Konkrétně se zajímáme o kterékoliv z následujících zranitelností:

- Cross-site request forgery (CSRF/XSRF)
- Cross-site scripting (XSS)
- Authentication bypass / unauthorised data access
- Encryption vulnerabilities
- Remote code execution
- Injection vulnerabilities
- Privilege escalation

Tento dokument není veřejným příslibem ani slibem odškodnění ve smyslu občanského zákoníku. Nevylučujeme však možnost rozhodnutí o odměně za nahlášení zranitelnosti, které bude pro společnosti MONETA přínosem, dle okolností daného případu.