Corporate Address
795 Commerce Dr, Ste 5
Venice, FL 34292

December 13, 2024

NH Department of Justice
Consumer Protection and Antitrust Bureau
1 Granite Place South
Concord, NH 03301
doj-cpb@doj.nh.gov

Dear Attorney General,

Pursuant to N.H. Rev. Stat. § 359-C:19 *et seq.*, we are writing to notify you of a data security incident involving approximately 182 New Hampshire residents.

IDENTIFICATION OF THE PARTIES

Byte Federal Inc. is a Florida corporation with headquarters located at 795 Commerce Dr Ste 5, Venice, FL 34292. The Company is a registered and licensed provider of money transmission services and other financial services to consumers in the United States and Australia. The person reporting this event to your office is Attorney Anessa Allen Santos who serves as General Counsel. The person responsible for the event is Mr. Lee Hansen, Chief Operating Officer and Chief Information Officer.

NATURE OF THE INCIDENT

On September 30, 2024, Byte Federal became aware of an unauthorized attempt to manipulate our database. However, there was no indication at the time that any customer information was at risk. We immediately blacklisted the attacker's public address. By 10:00 AM, we had identified the attacker's IP addresses leading to a temporary halt in operations and database lockdown. Further investigation revealed that the breach originated from a misconfiguration in our web server, which exposed a Personal Access Token in the .git/config file of our staging website. This token granted the attacker access to our GitLab code repository, allowing them to extract hardcoded data.

On October 2, 2024, we detected unauthorized access to our lightning server. The initial database attack was traced to an IP address (193.169.245.119) in Amsterdam, Netherlands, but we cannot confirm whether a VPN was used or the identity of the attacker. At this time, there was no indication that the attacks were related or that any customer data was compromised.

On November 18, 2024, we became aware of a phishing campaign wherein the attacker registered the domains bytefed.co and bytefederal.app and developed a phishing website mimicking our official site. On November 18, the attacker sent 573 phishing text messages via our Twilio account, directing customers to a fake "reward website". It was at this time we learned that customer data had been compromised. The attacker also issued a threat to release stolen data unless offered a "better deal than the black market" for our customer data. This prompted an immediate shutdown of our operations to quarantine the threat and measures to secure customer accounts and related data.

The categories of customer data that were compromised include

The data was encrypted, but the attacker also acquired the encryption key. We confirm that no customer funds or assets were lost, but we cannot confirm whether the data was sold on the dark web or otherwise shared. We have no way of knowing the attacker or their origin.

NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED

Approximately 58,000 customers were affected nationwide, 182 of whom are residents of New Hampshire. TransUnion has been retained to help send notice of the data breach to all affected residents in conformity with the requirements of N.H. Rev. Stat. § 359-C:19 *et seq.*. We expect this notice to go out in the next few business days. A copy of the template that TransUnion will use to deliver the notice is included.

STEPS WE HAVE TAKEN OR PLAN TO TAKE RELATING TO THE INCIDENT

Throughout the duration of the incident, we implemented several security measures:

- Global security token rotation
- Replacement of all compromised passwords and keys
- Implementation of IP restrictions and enhanced firewall rules
- Development of an internal security monitoring tool
- Continuous analysis of potential new attack vectors
- Forced reset of user account access
- Report the crime to the Sarasota County Sheriff's Office

Since the incident, we have retained a business intelligence and cybersecurity firm to conduct an external investigation and audit of our network protocols, policies, and procedures and to perform penetration testing and social engineering tests. Based on the results of this investigation, we expect to update our written information security program (WISP) to strengthen our systems and to conduct training of our staff to implement the updated WISP. We also retained the services of TransUnion to help deliver the data breach notification to affected residents of New Hamsphire.

CONTACT INFORMATION

For further information regarding this event, please feel free to contact Mr. Lee Hansen, CIO and COO. He can be reached via telephone at .

Sincerely,

Attorney Anessa Allen Santos
General Counsel

<Return Name>
c/o Cyberscout
<Return Address>
<City> <State> <Zip>

ByteFederal
Corporate Address
795 Commerce Dr., Ste 5
Venice, FL 34292

<FirstName> <LastName>
<Address1>
<Address2>
<City><State><Zip>

December x, 2024

RE: NOTICE OF DATA BREACH

Dear <<first name>> <<last name>>,

What Happened

On November 18, 2024, Byte Federal became aware of a security breach by a bad actor who gained unauthorized access to one of our servers by exploiting a vulnerability in software provided by a third party. Upon discovery of the incident, our team immediately shut down our platform, isolated the bad actor, and secured the compromised server. We also made immediate enhancements to our systems, security, and practices. For example, our team performed a hard reset on all customer accounts. We sent notice of the incident to our users via mail and we have issued a press release on our website with further detail. We have also updated all of our internal passwords, password management system, tokens and keys for our network to prevent any further unauthorized access. With the assistance of an independent cybersecurity team, we are conducting a forensic investigation to determine the cause and the scope of the incident. This investigation is ongoing, and we continue to cooperate with law enforcement in this regard. **No user funds or assets were compromised.**

What Information Was Involved

Customer personal information that was subject to the attempt at unauthorized access includes

However, we have no evidence at this time that any of your personal information was actually compromised or misused in any manner. Nonetheless, we are taking precautionary measures to ensure the security of your data and to help alleviate any concerns you may have.

What We Are Doing

If you have been impacted by this situation and require further assistance from us, you can reach us using our dedicated help line at or via email at s . Our customer service representatives are available Monday through Friday between the hours of 8:00 am to 10:00 pm EST and Saturday through Sunday 10 am to 6 pm EST. For ongoing updates from our investigation, please consult our website at w

What You Can Do

If you have not reset your login credentials for access to Byte Federal services, please do so now. It's important to remain vigilant for incidents of fraud and identity theft that may impact your financial security by regularly reviewing your account statements and by monitoring your credit reports. Under the Fair Credit Reporting Act, you have a right to obtain a free copy of your credit report from each of the three major credit bureaus once

every 12 months. You have the right to dispute incomplete or inaccurate information you find on your credit reports. You also have the right to know if information has been used against you, the right to limit access to your information and the right to seek damages.

You also have the right to place a fraud alert or security freeze on your account with each of the major credit reporting agencies which we strongly urge you to do. By placing a freeze, someone who fraudulently acquires your personal information will not be able to use it to open new accounts or borrow money in your name. If you are a victim of identity theft and have filed a report with your local law enforcement agency or submitted an ID Complaint Form with the FTC, it may be free to place the fraud alert and security freeze. To do so, please make direct contact with the agencies below. You may be asked to verify your personal information and to confirm your identity for your own protection.

Experian (1-888-397-3742)	**Equifax (1-800-525-6285)**	**TransUnion (1-800-680-7289)**
PO Box 4500	**PO Box 740241**	**PO Box 2000**
Allen, TX 75013	**Atlanta, GA 30374**	**Chester, PA 19016**
www.experian.com	www.equifax.com	www.transunion.com

Also, should you wish to obtain a credit report and monitor it on your own:

- **IMMEDIATELY** obtain free copies of your credit report and monitor them for unauthorized activity on the website www.annualcreditreport.com or by calling them toll-free at 1-877-322-8228. (Hearing impaired consumers can access TDD services at 1-877-730-4204.
- **Upon receipt of your credit report,** review it for suspicious activity.
- Be sure to promptly notify Byte Federal of any suspicious activity.

Other Important Information

If you suspect you may be a victim of identity theft, please report it to the FTC, your local law enforcement agency, and to your state Office of Attorney General. You can obtain more information from the Federal Trade Commission and your state Attorney General about identity theft and how to protect yourself. The FTC has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information on-line at www.ftc.gov/idtheft.

For residents of Massachusetts, you may receive a copy of the police report filed about this event upon written request made to the Byte Federal email shared above.

For residents of Maryland, you may reach the Maryland Attorney General online at www.marylandattorneygeneral.gov or by phone at 410-576-6300 / En español 410-230-1712 / 1-888-7430023 toll-free / TTY: Dial 7-1-1 or 800-735-2258.

For residents of North Carolina, you may reach the North Carolina Attorney General online at www.ncdoj.gov or by phone at 919-716-6000 / En español 919-716-0058.

At Byte Federal we take our responsibilities to protect your personal data very seriously. We are deeply troubled by this situation and apologize for any inconvenience.

Sincerely,

Paul Tarantino

Paul Tarantino
Byte Federal CEO