Hogan Lovells US LLP
Columbia Square
555 Thirteenth Street, NW
Washington, DC 20004
T +1 202 637 5600
F +1 202 637 5910
www.hoganlovells.com

December 16, 2020

By Electronic Mail

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
consumer@ag.iowa.gov

Re: Security Incident Notification

To Whom It May Concern:

I am writing on behalf of Paysafe Group Holdings Limited ("Company" or "Paysafe") to inform you of an incident that may have impacted personal information of 1,070 Iowa residents who established merchant accounts with the Company. Paysafe is an online payments company headquartered at 25 Canada Square, 27th Floor, London, United Kingdom E14 5LQ. The Company offers or has offered services branded as CHI Payments, iPayment, and Paysafe.

On November 6, 2020, the Company discovered a potential compromise of a website used by part of its U.S. business. The Company promptly initiated an investigation to determine the nature and potential impact of the vulnerability. In the course of doing so, the Company identified suspicious activity indicating that an unauthorized actor submitted automated queries to the website. The Company created a secure environment to test the queries, using available logs and other information to assess potential impact. On November 19, 2020, the Company determined that a subset of the queries identified might have involved data held on the website. The Company analyzed logs and other information available to assess whether those queries could have returned information to unauthorized actors, and engaged external forensics experts to assist. By December 3, 2020, the Company determined that some queries may have compromised certain information held on the website, although the evidence is not conclusive. At this time, the Company has identified evidence of suspicious activity on the website between May 13, 2018, and November 24, 2020. The Company has notified law enforcement.

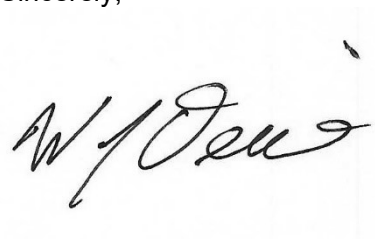
The information that may have been accessed includes names, contact details, Social Security numbers, and bank account information. The website did not hold customer transaction data, consumer data, or payment card information. The website impacted is separate from Paysafe's core processing and operating systems. After discovering the incident, the Company took steps to prevent further unauthorized access and has closed the website. Although the Company is not aware of any evidence confirming that the activity resulted in unauthorized actors acquiring or misusing personal information, the Company is notifying affected individuals out of an abundance of caution so that they can take steps to protect themselves. The Company continues to invest in cybersecurity and is enhancing its website scanning practices and vulnerability detection program.

On December 18, 2020, the Company will send notice by postal mail to the potentially impacted Iowa residents. We enclose a sample notice in this notification. In addition to providing information regarding credit reporting agencies,

security freezes, fraud alerts, and other identity theft prevention tools, the Company is offering credit monitoring and identity protection services for 2 years through Kroll to affected individuals, at no cost to them. The field for the phone number in the sample notice will be populated with the call center number: (833) 971-3287.

Please feel free to contact me if you have any questions or require additional information.

Sincerely,



James Denvil

Senior Associate
w.james.denvil@hoganlovells.com
D 1 202-637-5521

Enclosure

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

NOTICE OF DATA BREACH

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to inform you of a cybersecurity incident that may have affected personal information related to you. You provided the information to Merchant Services* in the course of enrolling for a merchant account.

WHAT HAPPENED

On November 6, 2020, through Merchant Services'* internal cybersecurity program, we discovered a potential compromise of a website used by part of our U.S. business. We promptly initiated an investigation to determine the nature and potential impact of the vulnerability. In the course of doing so, we identified suspicious activity indicating that an unauthorized actor submitted automated queries to the website. We created a secure environment to test the queries, using available logs and other information to assess potential impact. By November 19, 2020, we determined that a subset of the queries identified might have involved data held on the website. We analyzed logs and other information available to assess whether those queries could have returned information to unauthorized actors, and we engaged external forensics experts to assist. By December 3, 2020, we determined that some queries may have compromised certain information held on the website, although the evidence is not conclusive. At this time, we have identified evidence of suspicious activity on the website between May 13, 2018, and November 24, 2020. We have notified law enforcement. Although we are not aware of any evidence confirming that the activity resulted in unauthorized actors acquiring or misusing your personal information, we are providing this notice out of an abundance of caution so that you can take steps to protect yourself.

WHAT INFORMATION WAS INVOLVED

The information about you that may have been accessed includes your name, contact details, Social Security number, and bank account information. The website did not hold customer transaction data, consumer data, or payment card information. The website impacted is separate from Merchant Services'* core processing and operating systems. The website was part of a legacy system used internally and by a small group of former Chi Payment agents, a group acquired in an acquisition of iPayment in 2018, and contains certain data of a limited subset of merchants and agents.

WHAT WE ARE DOING

We take the privacy and security of your personal information seriously. After discovering the incident, we took steps to prevent further unauthorized access and have closed the website. We continue to invest in cybersecurity, including enhancing our website scanning practices and vulnerability detection program. Additionally, we have arranged for you to obtain credit monitoring and identity monitoring services at no cost to you for two years through Kroll, a leading provider of credit monitoring and identity monitoring services. Information regarding the package of services is included in Attachment 2 to this letter.

WHAT YOU CAN DO

We are not aware of any evidence indicating that your personal information has been misused or sold. Out of an abundance of caution, we recommend that you remain vigilant and review your financial records and statements for signs of suspicious activity. Please find additional information in Attachment 1 to this letter. As noted above, you can activate, at no cost to you, in the Kroll credit monitoring and identity monitroing services. Information about activation is contained in Attachment 2 to this letter.

*** Merchant Services includes, for purposes of this notification, CHI Payments, iPayment, and Paysafe.**

FOR MORE INFORMATION

If you have any questions or need additional information, please call 1-???-???-????, Monday through Friday from 8:00 am to 5:30 pm Central Time, excluding major U.S. holidays. Be prepared to provide your membership number: <<Member ID>>.

We apologize for any inconvenience this may cause.

Sincerely,

Merchant Services

Enclosures

Attachment 1: Additional Information

You should be cautious about using email to provide sensitive personal information, whether sending it yourself or in response to email requests. You should also be cautious when opening attachments and clicking on links in emails. Scammers sometimes use fraudulent emails or other communications to deploy malicious software on your devices or to trick you into sharing valuable personal information, such as account numbers, Social Security numbers, or usernames and passwords. The Federal Trade Commission (FTC) has provided guidance at https://www.consumer.ftc.gov/articles/0003-phishing.

You should review your financial statements and accounts for signs of suspicious transactions and activities. If you find any indication of unauthorized accounts or transactions, you should report the possible threat to local law enforcement, your State's Attorney General's office, or the FTC. If you are a resident of Rhode Island, you have the right to obtain a police report. You will find contact information for some of those entities below. If you discover unauthorized charges, promptly inform the relevant payment card companies and financial institutions.

Fraud Alert Information

Whether or not you enroll in the credit monitoring product offered, we recommend that you consider placing a free "Fraud Alert" on your credit file. Fraud Alert messages notify potential credit grantors to verify your identification before extending credit in your name in case someone is using your information without your consent. A Fraud Alert can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit. Fraud alerts last one year. Identity theft victims can get an extended fraud alert for seven years.

Call only one of the following three nationwide credit reporting companies to place your Fraud Alert: TransUnion, Equifax, or Experian. As soon as the credit reporting company confirms your Fraud Alert, they will also forward your alert request to the other two nationwide credit reporting companies so you do not need to contact each of them separately. You may also contact any of the consumer reporting agencies or the FTC for more information regarding fraud alerts. The contact information for the three nationwide credit reporting companies is:

Equifax	TransUnion	Experian
PO Box 740256	PO Box 2000	PO Box 9554
Atlanta, GA 30374	Chester, PA 19016	Allen, TX 75013
www.alerts.equifax.com	www.transunion.com/fraud	www.experian.com/fraud
1-800-525-6285	1-800-680-7289	1-888-397-3742

Free Credit Report Information

You have rights under the federal Fair Credit Reporting Act. These include, among others, the right to know what is in your credit file; the right to dispute incomplete or inaccurate information; and the right to ask for a credit score. Under federal law, you are also entitled to one free credit report once every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or make a request online at www.annualcreditreport.com.

Even if you do not find any suspicious activity on your initial credit reports, we recommend that you check your account statements and credit reports periodically. You should remain vigilant for incidents of fraud and identity theft. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency or state attorney general and file a police report. Get a copy of the report; many creditors want the information it contains to alleviate you of the fraudulent debts. You also should file a complaint with the FTC using the contact information below. Your complaint will be added to the FTC's Consumer Sentinel database, where it will be accessible to law enforcement for their investigations.

You may also contact the FTC at the contact information below to learn more about identity theft and the steps you can take to protect yourself. If you are a resident of the District of Columbia, Maryland, North Carolina, Iowa, Oregon, or Rhode Island, you can also reach out to your respective state's Attorney General's office at the contact information below. All other residents can find information on how to contact your state attorney general at www.naag.org/naag/attorneys-general/whos-my-ag.php.

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580
1.877.FTC.HELP (382.4357) / www.ftc.gov/idtheft

North Carolina Attorney General's Office
90001 Mail Service Center
Raleigh, NC 27699
1-919-716-6400 / https://ncdoj.gov/

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301
1-877-877-9392 / https://justice.oregon.gov

Office of the Attorney General for the District of Columbia
400 6th Street NW
Washington, D.C. 20001
1-202-727-3400 / oag.dc.gov

Maryland Attorney General's Office
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023 / www.marylandattorneygeneral.gov

Rhode Island Attorney General's Office
150 South Main Street
Providence, Rhode Island 02903
1-401-274-4400 / http://www.riag.ri.gov/

Consumer Protection Division
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, IA 50319
1-515-281-5926 / www.iowaattorneygeneral.gov

Security Freeze Information

You have the right to request a free Security Freeze (aka "Credit Freeze") on your credit file by contacting each of the three nationwide credit reporting companies via the channels outlined below. When a Credit Freeze is added to your credit report, third parties, such as credit lenders or other companies, whose use is not exempt under law will not be able to access your credit report without your consent. A Credit Freeze can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit. You may also contact any of the consumer reporting agencies or the FTC for more information regarding security freezes.

Equifax Security Freeze	TransUnion Security Freeze	Experian Security Freeze
PO Box 105788	PO Box 2000	PO Box 9554
Atlanta, GA 30348	Chester, PA 19016	Allen, TX 75013
www.freeze.equifax.com	www.transunion.com/freeze	www.experian.com/freeze
1-800-349-9960	1-888-909-8872	1-888-397-3742

To request a Credit Freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)

Attachment 2: Credit Monitoring and Identity Theft Services Enrollment Information

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

Visit **https://enroll.idheadquarters.com*** to activate and take advantage of your identity monitoring services.

*You have until **<<Date>>** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

* Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.