

April 5, 2019



Notice of Data Breach

We are writing to let you know of a security incident that involved your name and social security number. This incident did not occur at Harris Associates, rather it was the result of an attack on the systems of a third party Harris Associates uses to do business on your behalf, Instinet (Instinet Europe Limited and Instinet Global Services Limited). We are contacting you because of the importance of your relationship with us and because we take the protection and proper use of your personal information seriously. We have prepared the attached information which we hope you find helpful.


What Information Was Involved?

Your name and social security number were included in the information extracted from Instinet systems. Broker-dealers, like Instinet, require certain information about account holders for whom they execute trades to ensure compliance with tax requirements and other legal obligations. Instinet does not have access to your Harris Associates account number(s) or any of your contact information, including your address.

What Are We Doing?

Instinet has engaged a cybersecurity firm to assess and remediate the incident, and they notified authorities, including law enforcement. Since learning that this incident affected our clients, Harris Associates has been working with Instinet to understand the underlying incident and limit the potential impact to you.

In connection with this incident, Harris Associates is offering a 12-month subscription to identity theft protection services through ID Experts®, called MyIDCare™. If you are not already enrolled in this service or a similar service, we encourage you to register for this identity theft protection service which is available at no cost to you. You can enroll using the information in the box below:

<p style="text-align: center;">To Enroll, Please Call: 1-800-939-4170</p> <p style="text-align: center;">Or Visit: https://app.myidcare.com/account-creation/protect</p> <p style="text-align: center;">Enrollment Code: </p>

Your MyIDCare membership will include the following:

- Triple-Bureau Credit Monitoring,
- CyberScan Monitoring (monitoring of internet forums for your affected personal information)
- Full Managed ID Theft Restoration Services (assistance if you suspect your identity has been compromised)
- Identity Theft Insurance

What You Can Do

In addition to enrolling in MyIDCare, you can take the following steps to monitor for potential misuse of your personal information.

- Regularly review your account statements and monitor free credit reports.
- Under federal law, you are entitled to obtain one free copy of your credit report every twelve months from each of the nationwide consumer reporting agencies. You can obtain a free copy of your credit report from each agency by calling 1-877-322-8228 or visiting www.annualcreditreport.com. You can periodically obtain credit reports from each nationwide credit reporting agency. If you discover information on your credit report arising from a fraudulent transaction, you may request that the credit reporting agency delete that information from your credit report file.
- You may also consider contacting the credit reporting agencies directly if you wish to put in place a fraud alert or a security freeze. A fraud alert will notify any merchant checking your credit history that you may be the victim of identity theft and that the merchant should take additional measures to verify the application. Contacting any one of the three agencies will place an alert on your file at all three. A security freeze restricts all creditor access to your account but might also delay any requests you might make for new accounts. You may contact the nationwide credit reporting agencies at the following numbers to place a security freeze to restrict access to your credit report:
 - Equifax: 800-349-9960; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241
 - Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9554, Allen, TX 75013
 - TransUnion: 888-909-8872; transunion.com; Fraud Victim Assistance, P.O. Box 2000, Chester, PA 19022-2000

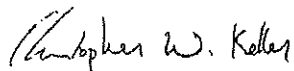
You will need to supply your name, address, date of birth, Social Security number, and other personal information. The agencies are not permitted to charge you for placing or lifting a freeze. Each credit reporting agency will confirm your request with a unique PIN or password that you will need in order to lift or remove the freeze. You should keep the PIN or password in a safe place.

- To report incidents of fraud and identity theft, you can contact the Federal Trade Commission (FTC) at 1-877-ID-THEFT, through their website at <http://identitytheft.gov>, or in writing to the Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20850.
- Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For More Information

On behalf of Harris Associates, we regret that this incident occurred and apologize for any inconvenience. We are committed to assisting you as needed and encourage you to contact [REDACTED] or [REDACTED] with any additional questions. Instinet also deeply regrets that this incident occurred and asked us to include the attached letter from them in this notice to you. If you would like to communicate with Instinet directly, you may contact Michelle Rodrigues, Instinet's Data Protection Officer, at eu.instinet.dpo@instinet.co.uk.

Sincerely,



Christopher W. Keller
Partner, Chief Operations Officer

2 April 2019

Dear Sir or Madam

Incident relating to personal data about you held on systems operated by Instinet Europe Limited and Instinet Global Services Limited (“Instinet”)

I am writing to inform you that Instinet was subjected to a security incident which led to the unauthorised access and extraction of certain data from Instinet’s desktop network by a third party. We responded immediately to the discovery of the incident, on 4 June 2018, by launching an investigation, engaging a leading cybersecurity firm to assess and remediate the incident and notifying appropriate authorities, including law enforcement.

It has since become apparent that certain information about you and other people connected to Instinet’s institutional clients may have been affected. As part of our ongoing investigation, we have now determined that unfortunately your name and social security number has been extracted during the incident.

We are continuing to take action to respond to the incident as described above in cooperation with appropriate authorities and law enforcement.

In addition to notifying you about this issue, we wanted to give you some guidance around the practical steps you can take to protect yourself. Steps you can take include the following:

- Remain vigilant and order credit reports regularly with a view to detecting suspicious activity on any accounts that you may have;
- Contact your personal bank to make them aware that personal data about you has been taken during a security incident and may be misused (in case anyone should, for example, try to make payments from your account including setting up an unauthorised direct debit or standing order);
- Register for identity protection and credit monitoring services to guard against the risk of identity theft or fraud. You can also monitor your own credit through the tips available at websites such as <https://www.annualcreditreport.com>, where a free credit report can be obtained every twelve months. If you think you have been a victim of fraud, you can report it to the Federal Bureau of Investigation (FBI); and
- Follow normal online hygiene by monitoring your personal email and social media accounts for any unusual activity (for example, for emails informing you that passwords used to access these accounts have been reset in circumstances where you have not requested this).

We deeply regret that this incident has affected you in this way. As mentioned above, we are working closely with law enforcement and third party specialists to ensure this incident is properly addressed.

For further information about this incident, please contact Michelle Rodrigues, our Data Protection Officer, using the following email address: eu.instinet.dpo@instinet.co.uk.

Yours faithfully

SIGNED for and on behalf of **Instinet Europe Limited and Instinet Global Services Limited**