



MULLEN  
COUGHLIN<sup>LLC</sup>  
ATTORNEYS AT LAW

RECEIVED  
MAR 09 2020  
CONSUMER PROTECTION

Ryan C. Loughlin  
Office: 267-930-4786  
Fax: 267-930-4771  
Email: rloughlin@mullen.law

1275 Drummers Lane, Suite 302  
Wayne, PA 19087

March 3, 2020

**INTENDED FOR ADDRESSEE(S) ONLY**

**VIA U.S. MAIL**

Consumer Protection Bureau  
Office of the New Hampshire Attorney General  
33 Capitol Street  
Concord, NH 03301

**Re: Notice of Data Event**

Dear Sir or Madam:

We represent Positec Tool Corporation (“Positec”) located at 10130 Perimeter Parkway Suite 300 Charlotte, North Carolina 28216, and are writing to notify your office of an incident that may affect the security of certain customer payment card information. The investigation into this matter is ongoing, and this notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Positec does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

**Nature of the Data Event**

On or about December 6, 2019, Positec observed suspicious activity on their e-commerce websites, [www.worx.com](http://www.worx.com) and [www.rockwelltools.com](http://www.rockwelltools.com). Positec immediately launched an investigation into this activity. Third-party forensic investigators assisted Positec with the investigation and its efforts to determine what happened and what information may be affected. The investigation identified code that was inserted into the checkout page and determined that this code was capable of collecting certain customer information when entered on the checkout page. Positec promptly removed the code at issue to prevent any further potential issues and confirmed the security of these websites. Customers can safely and securely use their payment card at [www.worx.com](http://www.worx.com) and [www.rockwelltools.com](http://www.rockwelltools.com).

On December 17, 2019, the investigation determined that Positec was the victim of a sophisticated cyber-attack that may have resulted in the code capturing certain customer information provided to make purchases on our e-commerce websites at certain times between December 6, 2019 and December 10, 2019.

Through this review Positec determined that the information that could have been subject to unauthorized access includes name, billing and shipping address, card holder name, credit card number, expiration date,

and CVV code for certain transactions on the [www.worx.com](http://www.worx.com) and [www.rockwelltools.com](http://www.rockwelltools.com) websites between December 6, 2019 and December 10, 2019.

### **Notice to New Hampshire Residents**

On or about March 3, 2020, Positec began providing written notice of this incident to affected individuals who provided payment card information on [www.worx.com](http://www.worx.com) and [www.rockwelltools.com](http://www.rockwelltools.com) between December 6 – December 10, 2019, which includes five (5) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

### **Other Steps Taken and To Be Taken**

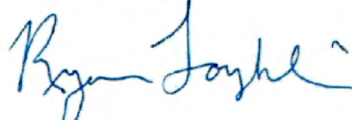
Upon discovering the event, Positec moved quickly to investigate and respond to the incident, assess the security of Positec systems, and notify potentially affected individuals. Positec is also working to review existing policies and procedures.

Additionally, Positec is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Positec is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

### **Contact Information**

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4786.

Very truly yours,



Ryan C. Loughlin of  
MULLEN COUGHLIN LLC

RCL: mef  
Enclosure

# **EXHIBIT A**



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

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
<<address\_1>>  
<<address\_2>>  
<<city>>, <<state\_province>> <<postal\_code>>  
<<country >>

**RE: Notice of Data Breach**

Dear <<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>,

Positec Tool Corporation (“Positec”) writes to inform you of a recent event that may impact some of your payment card information. We are providing you with information about the event, our response, and steps you may take to better protect against the possible misuse of your information, should you feel it appropriate to do so.

**What Happened?** On or about December 6, 2019, Positec observed suspicious activity on our e-commerce websites, www.worx.com and www.rockwelltools.com. Positec immediately launched an investigation into this activity. Third-party forensic investigators assisted Positec with the investigation and its efforts to determine what happened and what information may be affected. The investigation identified code that was inserted into the checkout page and determined that this code was capable of collecting certain customer information when entered on the checkout page. Positec promptly removed the code at issue to prevent any further potential issues and confirmed the security of our websites. You can safely and securely use your payment card at our websites.

On December 17, 2019, the investigation determined that Positec was the victim of a sophisticated cyber-attack that may have resulted in the code capturing certain customer information provided to make purchases on our e-commerce websites at certain times between December 6, 2019 and December 10, 2019.

**What Information Was Involved?** Your information was provided to Positec because of your consumer relationship with Positec. The investigation determined that the code could potentially have captured information including your name, billing and shipping address, card holder name, credit card number, expiration date, and CVV code for certain transactions between December 6, 2019 and December 10, 2019.

**What Are We Doing?** We take this incident and the security of your information seriously. Upon learning of this incident, we immediately took steps to address the issue and conducted an investigation to determine how this incident occurred and what information may be affected. To that end, we immediately removed the malicious codes, hardened the network environment and monitored for additional attempts to infiltrate the system. As part of our ongoing commitment to the privacy of personal information in our care, we are working to review our existing policies and procedures

**What You Can Do.** We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. If you see any unauthorized activity on your credit card statements, promptly contact your bank, credit union, or credit card company. You can find out more about how to help protect against potential identity theft and fraud in the enclosed *Steps You Can Take to Better Protect Your Information*.

**For More Information.** We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our assistance line at [1-800-833-8333](tel:1-800-833-8333), Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time.

Again, we take the privacy and security of the personal information in our care seriously, and sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

A handwritten signature in black ink that reads "Paul Tellefsen". The signature is written in a cursive style with a long horizontal stroke extending to the right.

Paul Tellefsen  
Chief Financial Officer

## **STEPS YOU CAN TAKE TO BETTER PROTECT YOUR INFORMATION**

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

<b>Experian</b> P.O. Box 9554 Allen, TX 75013 1-888-397-3742 <a href="http://www.experian.com/freeze/center.html">www.experian.com/freeze/center.html</a>	<b>TransUnion</b> P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 <a href="http://www.transunion.com/credit-freeze">www.transunion.com/credit-freeze</a>	<b>Equifax</b> P.O. Box 105788 Atlanta, GA 30348-5788 1-800-685-1111 <a href="http://www.equifax.com/personal/credit-report-services">www.equifax.com/personal/credit-report-services</a>
---	--	---

In order to request a security freeze, you will 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.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

<b>Experian</b> P.O. Box 2002 Allen, TX 75013 1-888-397-3742 <a href="http://www.experian.com/fraud/center.html">www.experian.com/fraud/center.html</a>	<b>TransUnion</b> P.O. Box 160 Woodlyn, PA 19094 1-800-680-7289 <a href="http://www.transunion.com/fraud-victim-resource/place-fraud-alert">www.transunion.com/fraud-victim-resource/place-fraud-alert</a>	<b>Equifax</b> P.O. Box 105069 Atlanta, GA 30348 1-888-766-0008 <a href="http://www.equifax.com/personal/credit-report-services">www.equifax.com/personal/credit-report-services</a>
---	--	--

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, [www.identitytheft.gov](http://www.identitytheft.gov), 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

**For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, [www.oag.state.md.us](http://www.oag.state.md.us).

**For North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, [www.ncdoj.gov](http://www.ncdoj.gov). You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

**For New Mexico residents**, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting [www.consumerfinance.gov/ff/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://www.consumerfinance.gov/ff/201504_cfpb_summary_your-rights-under-fcra.pdf), or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

**For New York residents**, the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

**For Rhode Island Residents**, the Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903; [www.riag.ri.gov](http://www.riag.ri.gov), 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. [There are two Rhode Island residents impacted by this incident.](#)