



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

NH DEPT OF JUSTICE
FEB 4 2022 PM 1:11

Alexander T. Walker
Office: (267) 930-4801
Fax: (267) 930-4771
Email: awalker@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

January 31, 2022

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 St. Clair County, IL (“St. Clair County”) located at 10 Public Square, Belleville, IL 62220 and are writing to notify your office of an incident that may affect the security of some personal information relating to one (1) New Hampshire resident. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, St. Clair County 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 May 30, 2021, St. Clair County became aware of anomalous and suspicious activities within its computer network. St. Clair County immediately launched an investigation with the assistance of third-party computer forensic specialists. The investigation determined that its computer network was infected with malware which caused a temporary disruption to certain services. On July 13, 2021, the investigation determined that an unknown actor gained access to the County’s systems on May 27, 2021 and removed certain files from the County’s computer systems on May 30, 2021. The County conducted a thorough and time-intensive review of the impacted files to determine if they contained sensitive information and identify address information for any potentially impacted individuals requiring notification. On December 6, 2021, the County completed its review and began coordinating notification to potentially impacted individuals.

The types of information involved for your state's residents may vary by individual and include name, address, and Social Security number.

Notice to New Hampshire Resident

On January 31, 2022, St. Clair County began providing written notice of this incident to potentially impacted individuals, which includes one (1) New Hampshire resident. 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, St. Clair County moved quickly to investigate and respond to the incident, assess the security of its systems, and notify potentially impacted individuals. St. Clair County is also working to implement additional safeguards and training to its employees. St. Clair County is providing access to credit monitoring services for twelve (12) months through Kroll to potentially impacted individuals, at no cost to these individuals.

Additionally, St. Clair County is providing potentially 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. St. Clair County 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) 930-4801.

Very truly yours,



Alexander T. Walker of
MULLEN COUGHLIN LLC

ATW/dle

Exhibit A



ST. CLAIR COUNTY BOARD

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

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

<<b2b_text_1(Variable Header)>>

Dear <<first_name>> <<last_name>>:

St. Clair County, IL (the "County") is writing to inform you of an incident that may affect the privacy of some of your information stored on County computer systems. This notice provides information about the incident, the County's response, and available resources to you to help protect your personal information from possible misuse, should you feel it necessary to do so.

What Happened?

On May 30, 2021, the County discovered anomalous and suspicious activities on its computer network. The County immediately launched an investigation with the assistance of third-party computer forensic specialists. The investigation determined that the County's computer network was infected with malware, which caused a temporary disruption to the County's services. The County also notified federal law enforcement. On July 13, 2021, the investigation determined that an unknown actor gained access to the County's systems on May 27, 2021 and removed certain files from the County's computer systems on May 30, 2021. The County reviewed these files to determine if they contain sensitive information. On December 6, 2021, the County completed that review and determined your information was contained within the impacted files.

What Information Was Involved?

The investigation determined that the following types of information relating to you were involved in this incident: <<b2b_text_2(data elements)>>.

What We Are Doing.

The County treats its responsibility to safeguard sensitive information as an utmost priority. As such, the County responded immediately to this incident and has been working diligently to provide you with an accurate and complete notice of the incident as soon as possible. As part of the ongoing commitment to the privacy and security of personal information in its care, the County is conducting a review of existing internal policies and procedures relating to data protection and security. The County is also implementing enhanced employee training protocols to better prevent future incidents. The County is providing notice of this incident to the impacted individuals and to regulators where required. As an added precaution, the County is providing you with access to complimentary identity monitoring services through Kroll for twelve (12) months.

What You Can Do.

The County encourages you to remain vigilant against incidents of identity theft and fraud and to review your account statements and explanation of benefits forms over the next 12 to 24 months and free credit reports for suspicious activity and to detect errors. The County also encourages you to review the *Steps You Can Take to Help Protect Your Information* section of this letter. You may also activate the offered identity monitoring services.

For More Information.

If you have additional questions, please call [1-800-244-7777](tel:1-800-244-7777), Monday through Friday, 8:00 am to 5:30 pm Central Time, excluding some U.S. holidays. You may also write to St. Clair County, IL at: #10 Public Square, Belleville, IL 62220.

Sincerely,

County of St. Clair

Steps You Can Take to Help Protect Personal Information

Activate Your Complimentary Identity Monitoring

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(ActivationDeadline)>> to activate your identity monitoring services.

Membership Number: <<MembershipNumber (S_N)>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

If you prefer to activate these services offline and receive monitoring alerts via the US Postal Service, you may activate via our automated phone system by calling 1-888-653-0511, Monday through Friday, 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number located in your letter ready when calling. Please note that to activate monitoring services, you will be required to provide your name, date of birth, and Social Security number through our automated phone system.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

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.

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.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit 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 three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit 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 credit 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 credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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.