



ELMORE COUNTY PROSECUTING ATTORNEY

SHONDI K. LOTT
PROSECUTING ATTORNEY

190 South 4th East
Mountain Home, Idaho 83647
Phone: (208) 587-2144 Ext. 503
Facsimile: (208) 587-2147
e-mail: prosecutor@elmorecounty.org

Lee Fisher
*Chief Deputy
Prosecuting
Attorney*

Ralph R. Blount
*Deputy Prosecuting
Attorney*

Elizabeth A. Harrison
*Deputy Prosecuting
Attorney*

Hayes Hartman
*Deputy Prosecuting
Attorney*

Philip R. Miller
*Deputy Prosecuting
Attorney*

December 14, 2022

Office of the Attorney General, State of Idaho
Deputy A.G. Brett Delange, Chief
Consumer Protection Division
P.O. Box 83720
Boise, Idaho 83720-0010
Via email to brett.delange@ag.idaho.gov

Re: Data Breach Notification per I.C. § 28-51-105

Dear Mr. Delange:

I am writing to you to notify you that Elmore County experienced a breach of the security of the system as defined in Idaho Code § 28-51-104(2) from one computer at the Elmore County Fair Grounds. The breach was discovered at about 9:30 AM on December 13, 2022. Per our IT Director, this computer has never been connected to the Elmore County or Sheriff's networks, does not have VPN access, and is completely isolated. The yet unidentified malicious actor apparently used the fairgrounds computer directly, possibly through a backdoor installed previously. County email address ecfair@elmorecounty.org was used to send a malicious email to approximately 490 outside email addresses, in addition to approximately 240 County email addresses. See Exhibit 1, attached. Additionally, the hack appears to have resulted in the release of employee and other persons' and entities personal identifying information. The emails sent were found in the Sent Items folder in Outlook and at 10:31 am. It could not be recalled. Therefore, our IT Director sent a warning notice to all recipients of the original malware/phishing email. See Exhibit 2, attached. About 200 emails sent to the email addresses affected by the malware/phishing scheme were undeliverable. The ecfair@elmorecounty.org email address has been placed on litigation hold to preserving any email that might be in the box and preventing deletions. The fairgrounds computer has been replaced and the offending computer held for forensic examination.

Our IT Director is Steve Van Norman. His contact information is:

Office: [208.587.2130 x1005](tel:208.587.2130)

Mobile: [208.605.8933](tel:208.605.8933)

svannorman@elmorecounty.org

On behalf of Elmore County Prosecutor Shondi K. Lott, thank you.

Ralph R. Blount
Ralph R. Blount
Deputy Prosecutor

Exhibit 1

fairgrounds grant

EC Elmore County Fair

To kelly@alaskacowboy.com; julielisle@rtci.net; jessica.castle@townsquareinteractive.com; amandamiller@townsquaremedia.com; burke@upstage-rentals.com; quickbooks-email@intuit.com; jc@jcmcdowell.com; hayseedphotography@hotmail.com; info@rodeonews.com; trishakepler96@hotmail.com; christy.lapp@townsquaremedia.com; +74 others

Bcc You tried to recall this message on Tuesday, December 13, 2022 10:45 AM.

Good Morning,

Julie Lisle has shared an important file with you securely for your review and signature.

[REVIEW/PRINT SECURED FILE](#)

Kindly return after signing for processing.

Julie Lisle
Elmore Co Fair and Rodeo
Fair Manager
855 E 1st Av
PO Box 205 Glenns Ferry, ID 83623

Exhibit 2

DO NOT CLICK - Fairgrounds Grant Link

Steve Van Norman <svannorman@elmorecounty.org>

To: Steve Van Norman; Bcc: Everyone


Good Morning,

If you've received an email from what appears to be Julie (efair), please DO NOT CLICK THE ATTACHED LINK.

I'll be heading down there momentarily to check her computer offline to see if she's infected. If not, someone has spoofed or hacked her email account, and I'll be taking care of that as well.

Thanks all...and if you clicked it, unplug your computer and call us.

Thanks!

 **Steve Van Norman**
IT Manager, Elmore County
Office: 208.587.2130 x1005 | Mobile: 208.605.8933
svannorman@elmorecounty.org
www.elmorecounty.org

IMPORTANT: The contents of this email and any attachments are confidential. They are intended for the named recipient(s) only. If you have received this email by mistake, please notify the sender immediately and do not disclose the contents to anyone or make copies thereof.