



Shelese McConnell <smcconnell@northbeachschools.org>

URGENT: Personal data breach notification

Shelese McConnell <smcconnell@northbeachschools.org>
To: All Staff <allstaff@northbeachschools.org>

Thu, Feb 1, 2018 at 8:50 AM

February 1, 2018

Good morning North Beach School District employees,

Last night we learned that there was a personal data breach in our district at approximately ten o'clock Tuesday, January 30. Someone posing as the superintendent requested via email a PDF listing of all employee names, addresses, salary information and social security numbers. The list included information for employees who received a W-2 form for the calendar year January 1, 2017 through December 31, 2017. Many districts across our state have been victims of this phishing scam, including Olympia School District.

We have contacted law enforcement, and our Technology Department is doing what it can to locate any possible information that could be helpful in an investigation.

We understand the severity of this issue and will deploy a privacy expert to advise employees on protective measures. We will deploy a system for employees to monitor their finances.

There are resources we will make available to you. However, we recommend initially that one option is for you to go to the Federal Trade Commission identitytheft.gov website to report an identity theft. You can follow the prompts from the Home page beginning with reporting the identity theft. Options available to you include requesting a free credit report and a credit freeze.

More information will be forthcoming as soon as we have additional information to share.

Thank you,

North Beach Business Services and Human Resources
360-289-2447



Shelese McConnell <smcconnell@northbeachschools.org>

RE: Update on Data Breach

Shelese McConnell <smcconnell@northbeachschools.org>

Thu, Feb 1, 2018 at 10:32 AM

To: All Staff <allstaff@northbeachschools.org>

RE: Update on Data Breach

Good morning North Beach School District employees,

This is an update of our initial notice regarding the personal data breach of employee information that occurred on at approximately ten o'clock a.m. on Tuesday, January 30. Someone posing as the superintendent requested via email a PDF listing of all employee names, addresses, salary information and social security numbers. The list included information for employees who received a W-2 form for the calendar year January 1, 2017 through December 31, 2017. Many districts across our state have been victims of this phishing scam, including Olympia School District.

We have contacted law enforcement, and the Internal Revenue Service. We also have notified our insurance carrier, which has provided us the following contact information for employees to seek assistance on protective measures and obtaining credit monitoring:

We also recommend you to go to the Federal Trade Commission identitytheft.gov website to report an identity theft. You can follow the prompts from the Home page beginning with reporting the identity theft. Options available to you include requesting a free credit report and a credit freeze. In addition, here are the toll-free numbers and addresses of the major credit reporting agencies

TransUnion Fraud Victim Assistance
P.O. Box 2000
Chester, PA 19016
1-800-680-7289
www.transunion.com

Experian:
P.O. Box 4500
Allen, TX 75013
1 888 397 3742
www.experian.com

Equifax:
Equifax Information Services LLC
PO Box 105069
Atlanta, GA 30348-5069
1 800 525 6285,
www.equifax.com

If you have further questions regarding this matter, please contact Shelese McConnell, 360-289-2447.
Thank you,

North Beach Business Services and Human Resources
360-289-2447



Shelese McConnell <smcconnell@northbeachschools.org>

UPDATE - BREACH

Shelese McConnell <smcconnell@northbeachschools.org>

Thu, Feb 1, 2018 at 11:43 AM

To: All Staff <allstaff@northbeachschools.org>

February 1, 2018

Good afternoon North Beach employees,

We have continued our research into our January 30th district data breach and wanted to update you on today's developments. There are two steps we recommend each employee take, as well as an important message from our payroll department.

First, today we met talked with special agents from the Department of the Treasury Internal Revenue Service Criminal Investigation department. Based on the specifics of this data breach, they recommend that as soon as possible, each employee files an IRS "Identity Theft Affidavit" form, which is attached. They also recommended we share with you the attached "Identity Theft" information sheet.

There are two attachments for you related to this first step.

Here is a description of the two attachments:

IRS Identity Theft: This is an information sheet that describes tax-related identity theft, as well as addresses steps for victims of tax-related identity theft. One of those steps is to complete IRS Form 14039, Identity Theft Affidavit.

IRS Form 14039, Identity Theft Affidavit: The IRS agents we talked with today encourage employees to fill out this form, regardless of whether or not they have already submitted their personal tax return with the IRS. The form may either be mailed or faxed, and a required fax cover sheet is attached for each employee to use when sending the form. We have notified school offices and support buildings throughout the school district to allow employees to use the district fax machines to fax the forms and required documentation (photocopy of a document to verify your identity) to the IRS. You may use a district copy machine to make a photocopy of the document to verify your identity.

Second, we will be providing you with information from our insurance company that will aid you in proceeding with credit monitoring services. Once we have that sign up information, it will be sent out immediately.

Payroll message

The following is important information from our payroll department:

"The data breach did not include the release of banking information related to your direct deposit account on file with the payroll department. However, if you make a change with your bank account, please notify payroll department immediately at 360-289-2447."

Again, we will continue to communicate with you as we learn more. Also, we

have created and are continuing to update a page of questions and answers about the data breach, that includes copies of these communications.

Thank you,

North Beach School District
Business Services and Human Resources
Shelese McConnell
(360) 289-2447

2 attachments

 **Identity Theft Information.pdf**
153K

 **Identity Theft Affidavit.pdf**
84K



Shelese McConnell <smcconnell@northbeachschools.org>

Data Breach

Shelese McConnell <smcconnell@northbeachschools.org>

Thu, Feb 1, 2018 at 4:41 PM

To: All Staff <allstaff@northbeachschools.org>

Dear North Beach Staff,

The data breach that occurred on January 30, 2018 was the result of an email phishing scam directed toward Human Resources/Payroll staff. The sender presented themselves as the superintendent and requested sensitive W2 and payroll information. I'm sorry that our district was targeted, and that personally identifiable information was shared through email. I reviewed the email on gmail and believed it was legitimate. I complied with that request. It was not until Superintendent Holcomb forwarded me an email sent by the ESD regarding this phishing scheme as an informational item that had impacted other districts that I realized this could have happened to us. I immediately contacted Superintendent Holcomb, who confirmed that she had not sent this email. Law enforcement was notified and we began steps to address this situation. I am deeply sorry that all of our personally identifiable information was compromised.

As mentioned in the email earlier today, the IRS urges *all* of our employees to fill out IRS Form 14039, Identity Theft Affidavit. The district will provide you with credit monitoring services, free of cost. We are waiting for activation codes. These should be out within 24 hours. We will email you as soon as we have the codes. Once you have the code, you will need to follow the step by step directions.

In the future, the district will provide more staff training on how to identify phishing scams. We will partner with our ESD and our data processing cooperative to identify and implement further preventive measures. I know this is a stressful situation for all of us and it will take some time to resolve. Thank you for your understanding.

Respectfully,
Shelese

Shelese McConnell

Business Manager
North Beach School District
360-289-2447 ext. 211



For Washington Schools, By Washington Schools

RECEIVED FEB 05 2018

February 1, 2018

Deborah Holcomb, Superintendent
North Beach School District
PO Box 159
Ocean Shores, WA 98569

RE: Insured: North Beach School District
Claim: Security Breach
Claim #: *47128
Date of Loss: 1/30/2018
Loss Location: Ocean Shores

This is to advise you James Costello has been assigned to handle the above-referenced claim on behalf of United Schools Insurance Program and North Beach School District. Please refer all inquiries, referencing the claim number, to the adjuster's attention at:

Toll free telephone #: (800) 407-2027
Phone #: (425) 260-1612
Fax #: (509) 754-3406
E-mail address: jcostello@chooseclear.com

/kes

cc: Martin-Morris Agency, Ephrata (by email)

The loss description shown is based upon information provided to Clear Risk Solutions. This acknowledgment does not confirm coverage for this claim. Coverage will be determined following a review of the policy and the facts and circumstances of the claim.

North Beach Phishing Scam

Police Case #: 18-1851

IRS ID of the Contact I talked to: 1000144468

Insurance Contact: Jim Costello

425-260-1612

jcostello@chooseclear.com

Insurance File #: 47128

Experian: 2 year monitoring service



Patrice Timpson <ptimpson@northbeachschools.org>

URGENT: Personal data breach notification

Shelese McConnell <smcconnell@northbeachschools.org>

Thu, Feb 1, 2018 at 8:50 AM

To: All Staff <allstaff@northbeachschools.org>

February 1, 2018

Good morning North Beach School District employees,

Last night we learned that there was a personal data breach in our district at approximately ten o'clock Tuesday, January 30. Someone posing as the superintendent requested via email a PDF listing of all employee names, addresses, salary information and social security numbers. The list included information for employees who received a W-2 form for the calendar year January 1, 2017 through December 31, 2017. Many districts across our state have been victims of this phishing scam, including Olympia School District.

We have contacted law enforcement, and our Technology Department is doing what it can to locate any possible information that could be helpful in an investigation.

We understand the severity of this issue and will deploy a privacy expert to advise employees on protective measures. We will deploy a system for employees to monitor their finances.

There are resources we will make available to you. However, we recommend initially that one option is for you to go to the Federal Trade Commission identitytheft.gov website to report an identity theft. You can follow the prompts from the Home page beginning with reporting the identity theft. Options available to you include requesting a free credit report and a credit freeze.

More information will be forthcoming as soon as we have additional information to share.

Thank you,

North Beach Business Services and Human Resources
360-289-2447



Patrice Timpson <ptimpson@northbeachschools.org>

RE: Update on Data Breach

Shelese McConnell <smcconnell@northbeachschools.org>

Thu, Feb 1, 2018 at 10:32 AM

To: All Staff <allstaff@northbeachschools.org>

RE: Update on Data Breach

Good morning North Beach School District employees,

This is an update of our initial notice regarding the personal data breach of employee information that occurred on at approximately ten o'clock a.m. on Tuesday, January 30. Someone posing as the superintendent requested via email a PDF listing of all employee names, addresses, salary information and social security numbers. The list included information for employees who received a W-2 form for the calendar year January 1, 2017 through December 31, 2017. Many districts across our state have been victims of this phishing scam, including Olympia School District.

We have contacted law enforcement, and the Internal Revenue Service. We also have notified our insurance carrier, which has provided us the following contact information for employees to seek assistance on protective measures and obtaining credit monitoring:

We also recommend you to go to the Federal Trade Commission identitytheft.gov website to report an identity theft. You can follow the prompts from the Home page beginning with reporting the identity theft. Options available to you include requesting a free credit report and a credit freeze. In addition, here are the toll-free numbers and addresses of the major credit reporting agencies

TransUnion Fraud Victim Assistance
P.O. Box 2000
Chester, PA 19016
1-800-680-7289
www.transunion.com

Experian:
P.O. Box 4500
Allen, TX 75013
1 888 397 3742
www.experian.com

Equifax:
Equifax Information Services LLC
PO Box 105069
Atlanta, GA 30348-5069
1 800 525 6285,
www.equifax.com

If you have further questions regarding this matter, please contact Shelese McConnell, 360-289-2447.
Thank you,

North Beach Business Services and Human Resources
360-289-2447



Patrice Timpson <ptimpson@northbeachschools.org>

UPDATE - BREACH

Shelese McConnell <smcconnell@northbeachschools.org>
To: All Staff <allstaff@northbeachschools.org>

Thu, Feb 1, 2018 at 11:43 AM

February 1, 2018

Good afternoon North Beach employees,

We have continued our research into our January 30th district data breach and wanted to update you on today's developments. There are two steps we recommend each employee take, as well as an important message from our payroll department.

First, today we met talked with special agents from the Department of the Treasury Internal Revenue Service Criminal Investigation department. Based on the specifics of this data breach, they recommend that as soon as possible, each employee files an IRS "Identity Theft Affidavit" form, which is attached. They also recommended we share with you the attached "Identity Theft" information sheet.

There are two attachments for you related to this first step.

Here is a description of the two attachments:

IRS Identity Theft: This is an information sheet that describes tax-related identity theft, as well as addresses steps for victims of tax-related identity theft. One of those steps is to complete IRS Form 14039, Identity Theft Affidavit.

IRS Form 14039, Identity Theft Affidavit: The IRS agents we talked with today encourage employees to fill out this form, regardless of whether or not they have already submitted their personal tax return with the IRS. The form may either be mailed or faxed, and a required fax cover sheet is attached for each employee to use when sending the form. We have notified school offices and support buildings throughout the school district to allow employees to use the district fax machines to fax the forms and required documentation (photocopy of a document to verify your identity) to the IRS. You may use a district copy machine to make a photocopy of the document to verify your identity.

Second, we will be providing you with information from our insurance company that will aid you in proceeding with credit monitoring services. Once we have that sign up information, it will be sent out immediately.

Payroll message

The following is important information from our payroll department:

"The data breach did not include the release of banking information related to your direct deposit account on file with the payroll department. However, if you make a change with your bank account, please notify payroll department immediately at 360-289-2447."

Again, we will continue to communicate with you as we learn more. Also, we have created and are continuing to update a page of questions and answers about the data breach, that includes copies of these communications.

Thank you,

North Beach School District
Business Services and Human Resources
Shelese McConnell
(360) 289-2447

2 attachments



Identity Theft Information.pdf
153K



Identity Theft Affidavit.pdf
84K



Identity Theft Information for Taxpayers



Identity theft places a burden on its victims and presents a challenge to many businesses, organizations and governments, including the IRS. The IRS combats this crime with an aggressive strategy of prevention, detection and victim assistance.

What is tax-related identity theft?

Tax-related identity theft occurs when someone uses your stolen Social Security number (SSN) to file a tax return claiming a fraudulent refund. If you become a victim, we are committed to resolving your case as quickly as possible.

You may be unaware that this has happened until you e-file your return and discover that a return already has been filed using your SSN. Or, the IRS may send you a letter saying it has identified a suspicious return using your SSN.

Know the warning signs

Be alert to possible tax-related identity theft if you are contacted by the IRS about:

- More than one tax return was filed for you,
- You owe additional tax, have a refund offset or have had collection actions taken against you for a year you did not file a tax return, or
- IRS records indicate you received wages or other income from an employer for whom you did not work.

Steps for victims of identity theft

If you are a victim of identity theft, the Federal Trade Commission recommends these steps:

- File a complaint with the FTC at identitytheft.gov.
- Contact one of the three major credit bureaus to place a 'fraud alert' on your credit records:
 - www.Equifax.com 1-888-766-0008
 - www.Experian.com 1-888-397-3742
 - www.TransUnion.com 1-800-680-7289
- Close any financial or credit accounts opened by identity thieves

If your SSN is compromised and you know or suspect you are a victim of tax-related identity theft, the IRS recommends these additional steps:

- Respond immediately to any IRS notice; call the number provided.
- Complete IRS [Form 14039, Identity Theft Affidavit](#), if your e-file return rejects because of a duplicate filing under your SSN or you are instructed to do so. Use a fillable form at IRS.gov, print, then attach form to your paper return and mail according to instructions.

- Continue to pay your taxes and file your tax return, even if you must do so by paper.
- If you previously contacted the IRS and did not have a resolution, contact us for specialized assistance at 1-800-908-4490. We have teams available to assist.

More information is available at: IRS.gov/identitytheft or FTC's identitytheft.gov.

About data breaches and your taxes

Not all data breaches or computer hacks result in tax-related identity theft. It's important to know what type of personal information was stolen.

If you've been a victim of a data breach, keep in touch with the company to learn what it is doing to protect you and follow the "Steps for victims of identity theft." Data breach victims should submit a Form 14039, *Identity Theft Affidavit*, only if your Social Security number has been compromised and IRS has informed you that you may be a victim of tax-related identity theft or your e-file return was rejected as a duplicate.

How you can reduce your risk

Join efforts by the IRS, states and tax industry to protect your data. Taxes. Security. Together. We all have a role to play. Here's how you can help:

- Always use security software with firewall and anti-virus protections. Use strong passwords.
- Learn to recognize and avoid phishing emails, threatening calls and texts from thieves posing as legitimate organizations such as your bank, credit card companies and even the IRS.
- Do not click on links or download attachments from unknown or suspicious emails.
- Protect your personal data. Don't routinely carry your Social Security card, and make sure your tax records are secure.

See [Publication 4524, Security Awareness for Taxpayers](#) to learn more.

NOTE: The IRS does not initiate contact with taxpayers by email to request personal or financial information. This includes any type of electronic communication, such as text messages and social media channels.

Section E – Representative, Conservator, Parent or Guardian Information (Required if completing Form 14039 on someone else's behalf)

Check only **ONE** of the following five boxes next to the reason you are submitting this form

- 1. The taxpayer is deceased and I am the surviving spouse**
 - No attachments are required, including death certificate.
- 2. The taxpayer is deceased and I am the court-appointed or certified personal representative**
 - Attach a copy of the court certificate showing your appointment.
- 3. The taxpayer is deceased and a court-appointed or certified personal representative has not been appointed**
 - Attach copy of death certificate or formal notification from a government office informing next of kin of the decedent's death.
 - Indicate your relationship to decedent: Child Parent/Legal Guardian Other _____
- 4. The taxpayer is unable to complete this form and I am the appointed conservator or have Power of Attorney/Declaration of Representative authorization per IRS Form 2848**
 - Attach a **copy** of documentation showing your appointment as conservator or POA authorization.
 - If you have an IRS issued **Centralized Authorization File (CAF)** number, enter the nine-digit number:

--	--	--	--	--	--	--	--	--
- 5. The person is my dependent child or my dependent relative**

By checking this box and signing below you are indicating that you are an authorized representative, as parent, guardian or legal guardian, to file a legal document on the dependent's behalf.

 - Indicate your relationship to person: Parent/Legal Guardian Fiduciary Relationship per IRS Form 56
 Power of Attorney Other

Representative's name

Last name	First name	Middle initial
-----------	------------	----------------

Representative's current mailing address (City, town or post office, state, and ZIP code)

Representative's telephone number

Instructions for Submitting this Form

Submit this completed and signed form to the IRS via **Mail** or **FAX** to specialized IRS processing areas dedicated to assist you. In **Section C** of this form, be sure to include the Social Security Number in the 'Taxpayer Identification Number' field.

Help us avoid delays:

- Choose one method of submitting this form either by Mail or by FAX, not both.
- Please provide clear and readable photocopies of any additional information you may choose to provide.
- Note that 'tax returns' may not be submitted to either the mailing address or FAX number.

Submitting by Mail	Submitting by FAX
<ul style="list-style-type: none"> • If you checked Box 1 in Section B in response to a notice or letter received from the IRS, return this form and if possible, a copy of the notice or letter to the address contained in the notice or letter. • If you checked Box 1 in Section B of Form 14039, are unable to file your tax return electronically because the primary and/ or secondary SSN was misused, attach this Form 14039 to the back of your paper tax return and submit to the IRS location where you normally file your tax return. • If you've already filed your paper return, please submit this Form 14039 to the IRS location where you normally file. Refer to the 'Where Do You File' section of your return instructions or visit IRS.gov and input the search term 'Where to File'. • If you checked Box 2 in Section B of Form 14039 (no current tax-related issue), mail this form to: <div style="text-align: center;"> Department of the Treasury Internal Revenue Service Fresno, CA 93888-0025 </div> 	<ul style="list-style-type: none"> • If you checked Box 1 in Section B of Form 14039 and are submitting this form in response to a notice or letter received from the IRS. If it provides a FAX number, you should send there. If no FAX number is shown on the notice or letter, please follow the mailing instructions on the notice or letter. • Include a cover sheet marked 'Confidential'. • If you checked Box 2 in Section B of Form 14039 (no current tax-related issue), FAX this form toll-free to: <div style="text-align: center;"> 855-807-5720 </div>

Privacy Act and Paperwork Reduction Notice

Our legal authority to request the information is 26 U.S.C. 6001. The primary purpose of the form is to provide a method of reporting identity theft issues to the IRS so that the IRS may document situations where individuals are or may be victims of identity theft. Additional purposes include the use in the determination of proper tax liability and to relieve taxpayer burden. The information may be disclosed only as provided by 26 U.S.C. 6103. Providing the information on this form is voluntary. However, if you do not provide the information it may be more difficult to assist you in resolving your identity theft issue. If you are a potential victim of identity theft and do not provide the required substantiation information, we may not be able to place a marker on your account to assist with future protection. If you are a victim of identity theft and do not provide the required information, it may be difficult for IRS to determine your correct tax liability. If you intentionally provide false information, you may be subject to criminal penalties. You are not required to provide the information requested on a form that is subject to the Paperwork Reduction Act unless the form displays a valid OMB control number. Books or records relating to a form or its instructions must be retained as long as their contents may become material in the administration of any Internal Revenue law. Generally, tax returns and return information are confidential, as required by section 6103. Public reporting burden for this collection of information is estimated to average 15 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. If you have comments concerning the accuracy of these time estimates or suggestions for making this form simpler, we would be happy to hear from you. You can write to the Internal Revenue Service, Tax Products Coordinating Committee, SE:W:CAR:MP:T:T:SP, 1111 Constitution Ave, NW, IR-6526, Washington, DC 20224. Do not send this form to this address. Instead, see the form for filing instructions. Notwithstanding any other provision of the law, no person is required to respond to, nor shall any person be subject to a penalty for failure to comply with, a collection of information subject to the requirements of the Paperwork Reduction Act, unless that collection of information displays a currently valid OMB Control Number.



Patrice Timpson <ptimpson@northbeachschools.org>

IRS Cover Sheet

Shelese McConnell <smcconnell@northbeachschools.org>

Fri, Feb 2, 2018 at 12:27 PM

To: All Staff <allstaff@northbeachschools.org>

Hello All,

The cover sheet that goes with the IRS form I sent yesterday is a normal fax sheet. You can use the one in the office at each school.

Thanks,

Shelese McConnell

Business Manager

North Beach School District

360-289-2447 ext. 211



Patrice Timpson <ptimpson@northbeachschools.org>

Fraud Monitoring Activation

Shelese McConnell <smcconnell@northbeachschools.org>
To: All Staff <allstaff@northbeachschools.org>

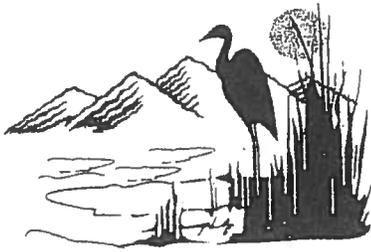
Fri, Feb 2, 2018 at 4:13 PM

Hello,

The Fraud Monitoring forms have been emailed out and will be mailed out.
There is an activation code in the form, along with instructions on how to get set up.

Thank you,

Shelese McConnell
Business Manager
North Beach School District
360-289-2447 ext. 211



North Beach School District No. 64

2652 State Route 109, Ocean City • PO Box 159

Ocean Shores, WA 98569

360) 289-2447 • (360) 289-2492 Fax

February 2, 2018

RE: Important Security Notification
Please read this entire letter.

Dear [REDACTED],

We are contacting you regarding a data security incident that has occurred on January 30, 2018 at North Beach School District. This incident involved your 2017 W-2 information, including your social security number. As a result, your personal information may have been potentially exposed to others. Please be assured that we have taken every step necessary to address the incident.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this offer is available to you for two-years from the date of this letter and does not require any action on your part at this time.

The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

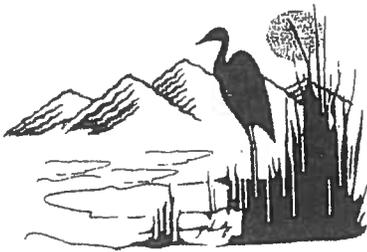
While Identity Restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorksSM as a complimentary two-year membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: May 31, 2018** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bplus>
- Provide your **activation code:** [REDACTED]

If you have questions about the product, need assistance with identity restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332 by **May 31, 2018**. Be prepared to provide engagement number **DB05239** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.



North Beach School District No. 64

2652 State Route 109, Ocean City • PO Box 159

Ocean Shores, WA 98569

360) 289-2447 • (360) 289-2492 Fax

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information.

We sincerely apologize for this incident and regret any inconvenience it may cause you. Should you have questions or concerns regarding this matter, please do not hesitate to contact us at (360) 289-2447.

Sincerely,

Deborah Holcomb
Superintendent

* Offline members will be eligible to call for additional reports quarterly after enrolling

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions