Appendix

AmeriCommerce recently completed an investigation relating to their e-commerce application. AmeriCommerce identified a security incident on March 29, 2021 involving unauthorized use of the file upload feature of the AmeriCommerce application to add code to the checkout page of some of its merchant customers. A cybersecurity firm was engaged to assist with a forensic investigation. Findings from the investigation determined that code was added to the sites involved at different times starting on March 25, 2021, and the code was removed from all sites on March 29, 2021. While the unauthorized code was present on the websites, it was capable of copying the following information entered by customers during the checkout process on the merchant's website: name, shipping and billing address, email address, phone number, payment card number, expiration date and CVV.

At the conclusion of the investigation, AmeriCommerce notified the involved merchants and offered to provide notification to individuals and regulators on behalf of the merchants. Beginning on April 23, 2021, AmeriCommerce began mailing notification letters via U.S. mail to the 28 Maine residents involved. An exemplar of the notification letters is enclosed with this letter. A list of merchants that have opted-in to AmeriCommerce's notification is also enclosed with this notice.

The notification provided to individuals encouraged them to review their payment card account statements for any unauthorized charges and to immediately notify the issuing bank of any discrepancies. AmeriCommerce also established a dedicated, toll-free call center where individuals may obtain more information regarding the incident.

Involved Merchants

4TecDirect
7ENT
AccurateDiesel
AllSafeIndustries
AlphaTechpet
AWildSoapBar
BakersSport
BestOfBigRed
BodyAsDoctor
CablesDirect
CaravanBeads
ClassicEnt
CoinSupplyExpress
Cospheric
CougarPartsCatalog
CrawlSpaceRepair
CritterFence
CSTactical
DecoSealers
DeiEquipment
directdeals
DirectLighting
DogFoodDirect
DraftingSuppliesDew
DrJsupplements
EarthDog
ElectricalBasics
EMarineInc
EonPro
Eurway
ExtremeGlow
FireHoseDirect
GamblersOasisUSA
HealthAndWisdom
HerbsFirst
HighPointGifts
HollandBulbFarms
IAPrisonInd
IrishSisters
JarmazingProducts
JollyStoreCrafts
KKOrchid
MartinRFSupply
MaryJanesFarm
MassageKing
MCARBO
Mearicle
MilkReclamationBarn
Mindkits
MosFudgeFactor
Mototote
MovieZyng
MunrosSafety
NationalFirefighter
NaturesHead
OldWillKnottScales
OrangeArtStore
PacificCoastSunglasses
PaperrollsNMore
Petagree
PhoenixLearningResources
PiTapeTexasLLC
PlaybillStore
pleasantsmoke
PondAlgaeSolutions
PrecisionRaceworks
PuppyCake
PureLifeMinistries
QualityTapestries
RacerXFabrication
RealEstateSchoolOfSC
ReplacementDecals
Rochester100
rofentsllc
RoofRake
SeattleCoffeeWorks
ShellLumber
ShipleysOutdoors
ShopBretMichaels
StoneCareCentral
SupremeCapAndGown
TRUSupply
TSDistributors
Tunatuna
VaporBrothers
VaporWarehouse
VeltonsCoffee
VibratorWarehouse
WeSpeakWine
WholeTiles
WiringDepot

AmeriCommerce
268 Pearl St, Beaumont, TX 77701

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

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

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

AmeriCommerce is writing to let you know that we recently identified and addressed an incident that may have involved your payment card information. This notice explains the incident, the measures we have taken in response, and additional steps you may consider taking.

What Happened?

AmeriCommerce is an e-commerce technology company that helps merchants process payment card transactions. We identified a security incident on March 29, 2021 involving unauthorized use of the file upload feature of the AmeriCommerce application to add code to the checkout page of some of our merchant customers, including a merchant you made a purchase from <<b2b_text_1(MerchantName)>>. The code was added to the sites involved at different times starting on March 25, 2021, and we removed the code from all sites on March 29, 2021. Transactions using a stored payment card and transactions entered directly by the merchant were not involved. We are notifying you because you placed an order during a time when the unauthorized code was present.

What Information Was Involved?

The information entered during the checkout process that could have been obtained by the code includes your name, address, email address, payment card number, expiration date, and the external verification code for the credit card ending in <<b2b_text_2(LastDigits)>>.

What We Are Doing.

In addition to conducting an investigation, we notified law enforcement and implemented additional security measures to secure the AmeriCommerce platform. We also notified the payment card networks so that they can inform the banks that issued the cards.

What You Can Do.

We encourage you to closely review your payment card account statements for any unauthorized charges. You should immediately report any unauthorized charges to the bank that issued your card because payment card network rules generally provide that cardholders are not responsible for unauthorized charges that are timely reported. Please see the additional information attached to this letter for additional steps you may take.

For More Information.

We regret that this occurred and apologize for any inconvenience. If you have any further questions or concerns, we established a dedicated call center, which can be reached by calling 1-XXX-XXX-XXXX, Monday through Friday from 8:00 a.m. – 5:30 p.m. Central Time, excluding major U.S. holidays.

Sincerely,

Jack Cravy
Vice President

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Additional information for residents of the following states:

Connecticut: You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office*, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

Rhode Island: This incident involves 16 individuals in Rhode Island. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

West Virginia: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

New Mexico: A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- 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 reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a 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.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.