

KNOWLEDGE EXCHANGE PARTNER

VOLUME 14 | ISSUE 9 | SEPTEMBER 2020

THIS ISSUE:

Steering Clear of Scams 1

International Trade Update 4

Editor: Chris Laughton
Chris.Laughton@FarmCreditEast.com

Contributors:
Deanna Pellegrino
Tom Cosgrove
Chris Laughton

Steering Clear of Scams

Written by Deanna Pellegrino, Farm Credit East Information Security Specialist

The world of cyber security can be scary. With hacking, identity theft, fraud, phishing and other scams so prevalent, sometimes it can seem overwhelming. Although new threats are always on the rise, many scams can be avoided with a bit of knowledge and caution on your part.

Phishing

One common type of scam is called “phishing.” Phishing is an attempt by computer hackers to infiltrate your device or network via deceptive emails which often contain malicious links or software. Like actual fishing, these people often cast a broad net and then wait to see who “bites” or responds. Clicking on links or attachments in phishing emails could allow hackers access to your system or expose personal information. While all too common, and potentially dangerous, many phishing attempts are easy to spot if you know what to look for. Here are a few warning tips:


- Be wary of personal messages from people you don’t know, or business emails from companies you don’t do business with.
- Be aware that you can’t always trust the name the email appears to be from — email addresses can be “spoofed” — meaning a hacker sending the message pretends to be someone else, maybe someone you know. Hovering over the email is one way to identify the senders actual email address, but in any case, if an email looks like it’s from one of your contacts, but seems strange, double check to make sure it’s legitimate.
- Poor spelling and grammar are major red flags. Everyone makes the occasional mistake, but phishing emails are often riddled with misspellings and other basic errors.
- Note that links contained in emails may not always be what they seem. The text containing the link might say one thing, but actually take you somewhere else. Hovering over the link will often show the destination URL. If it doesn’t match what it is supposed to, don’t click on it.
- Remember the old adage, “If it seems too good to be true, it probably is.” It’s unlikely you’ve won a contest you don’t remember entering, received an inheritance from an unknown relative, or been granted a windfall from some mysterious government program. Free software can be risky as well. Some apps or programs offered for free on the internet are loaded with bugs and malware.

“While all too common, and potentially dangerous, many phishing attempts are easy to spot if you know what to look for.”

- Some scammers prey on people's fears and may couple this with a claim of urgency to get you to act quickly without second-guessing your actions. A particularly insidious type of scam is an email suggesting that you have been hacked (or your computer is infected) and the sender wants you to do something (click a link, download something, make a call, send Bitcoin, gift cards or do something else) in order to remove a virus or prevent some kind of negative outcome. This is rarely the case. They are exploiting your fears to lure you into their trap.
- Another sneaky deception is an email telling you that your password or account has been compromised (or expired), and that you need to click on a link to verify it or change it. In reality, the link might take you to a fraudulent website where they collect your login credentials. These can be tricky, and hackers will often include official logos they have copied off the internet, or otherwise try to make the email appear genuine. Unless you are certain that the message is genuine, it's a good practice to go to the business's known website address and log in there, rather than using links.


Below are two examples of phishing attempts with labels on suspicious pieces of the email that can help you identify when you're being phished.

Order Error and finances removed


OzuhejYmuk <ozuhejymuk@byt.im>
 Suspicious email address

To: Rackliffe, Scott

Retention Policy: 7 Year Data Retention (7 years) Expires: 07/20/2027


MyStatement.docx
 10 KB
 Unexplained attachment

Caution: External email

Hi there,

I'm sending this message to argue a charge in the amount of \$119 on my member's account. I recently bought the merchandise through when I looked at my banking account the identical amount has been cashed out from my credit card.


I am asking for that malfunction be corrected, that any finance charges associated with the disputed statement.

Attached are duplicates of my financial report and also the purchase info. Please fix the mistake promptly

All the best,
Micah Santos

Sender does not match email address – and do you know this person?
Does the message make sense?


Payment Advice – Ref:[GB183748292084] / Priority payment


no_replycustomerservice <no.replycustomerservice@securebankingservices.com>
 "securebankingservices" is not a legitimate company name

To: Rackliffe, Scott

Retention Policy: 7 Year Data Retention (7 years) Expires: 07/20/2027

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.


T1000394859483.docx
 10 KB
 Suspicious attachment

Caution: External email

Dear Sir/Madam,

The attached payment advice is issued at the request of our customer.

The advice is for your customer.

The payment was cancelled due to a wrong SWIFT code. Please check the attached and reconfirm your swift code as soon as possible.

Yours faithfully,
Global Payments and Cash Management
HSBC

Not addressed to you
"customer" not named
Message includes misspellings
False sense of urgency
Is this a company you do business with?

Passwords

Using secure passwords is crucial in keeping data safe! Almost everything you do online requires a password, and it can be very confusing keeping track of them all. Here are a few tips to keep your passwords secure to ensure unauthorized parties cannot reach your sensitive information:

- For most people, some usernames and passwords are more critical to keep secure than others. For example, the password to log in to your favorite restaurant to order takeout online is less critical than the password for your investment accounts. For those critical accounts, here are a few best practices:
 - Use unique passwords for each key account. That way, if your Netflix account is compromised, the hacker doesn't have your bank account password as well.
 - Consider using a secondary email for low-priority accounts, to keep your primary accounts more secure.
- Longer passwords are always better, as are those containing numbers or special characters. Try thinking of a sentence or phrase that is important to you and use those characters as your password. Example: You miss 100% of the shots you do not take translates to Ym100%otsydnt.
- If an account or password is compromised, change the log in credentials immediately and don't use them again. One way to find out about at least some data breaches is Firefox Monitor (monitor.firefox.com). You can enter your email address and it will tell you if it finds it connected to any known data breaches.

Identity Theft

Be extremely careful with your Social Security number (SSN). There are certainly legitimate reasons why some businesses may need it, such as banks, government authorities and others. Typically applying for credit will require your SSN as well. However, be careful if entering it on a website. Be certain you are on a secure site (look for "https://" in the address, or a padlock icon, in some browsers). If a hacker gains access to your SSN, there is a lot they can do, including applying for credit or loans in your name, unemployment compensation, making bank transfers, stealing tax refunds, and more. Pay attention to your mail and your credit report. (You can get it free online at AnnualCreditReport.com, and yes, they will need your SSN to access it. You can get a free copy every 12 months from each of the three main credit bureaus. One trick is to request one of them every four months to space them out.)

Phone Scams

Finally, there are phone scams. Be aware that the IRS, Social Security Administration or other federal agencies do not initiate contact with taxpayers by phone (or social media) to request personal or financial information, nor will they call and threaten to arrest you or seize your bank accounts.

Just as with e-mail "from" addresses, caller's phone numbers can be "spoofed" – and callers can pretend to be someone else. If a call from a company or government agency seems suspicious, hang up and call them back at a known number.

Stay vigilant!

Yes, it's a scary world out there and there are plenty of people who would like to use your personal information for their gain. However, a dose of healthy skepticism will serve you better than paranoia. Most scams and identity theft attempts can be thwarted with a bit of caution.

For more information on how to avoid phishing and other scams, please access Farm Credit East's [Customer Assistance Program](#). This is a confidential, free resource available to all Farm Credit East customers that provides information related to personal finance, human resources, wellness, and many more topics, including how to protect yourself from cyber attacks and scams.

International Trade Update

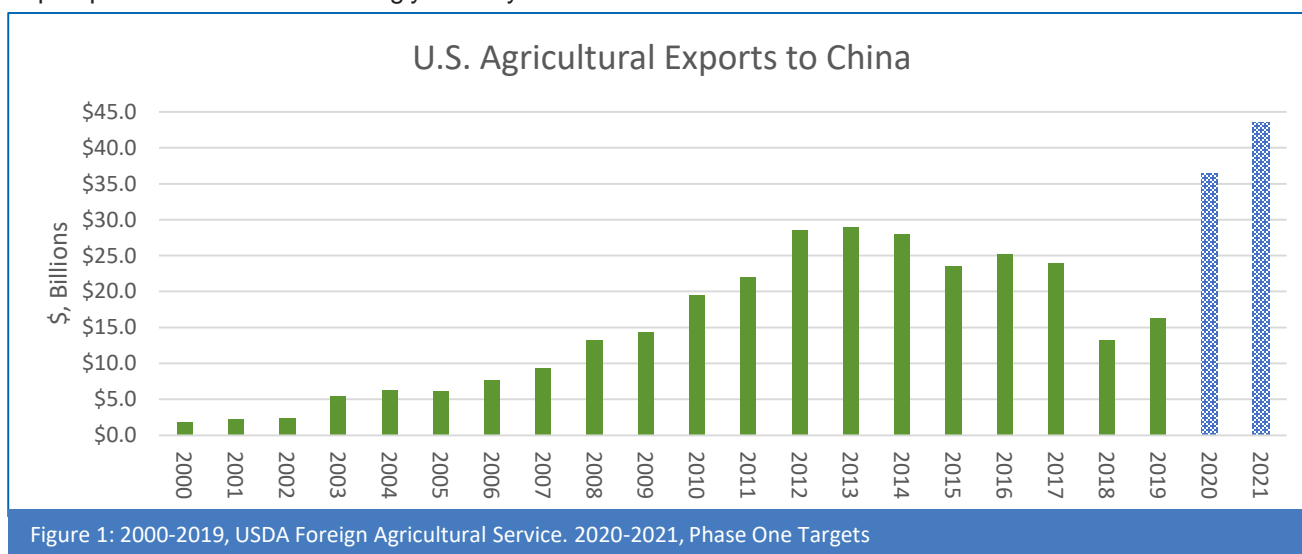
International trade has been a major issue affecting U.S. agriculture in recent years. The U.S. has had contentious relationships with several major trading partners around the world resulting in a roller coaster of news and developments around global trade, which has been further complicated in recent months by the COVID-19 pandemic. Agriculture, as one of the U.S.'s most significant export industries, has often been significantly affected by these developments.

Perhaps the most rocky international relationship the U.S. currently has is with China. Relations between the world's two largest economies and major trading partners have deteriorated with issues of contention, including the COVID-19 pandemic, the fate of Hong Kong, sanctions against Xinjiang over alleged human rights abuses, and technology issues, such as proposed U.S. bans on the apps TikTok and WeChat.

Beijing's commerce ministry announced on August 20 that the two sides would talk "in coming days," after President Trump postponed further discussions on the Phase One trade deal because he was unhappy with China's handling of the coronavirus. China appears to hold hope that the upcoming trade talks, agreed upon when the Phase One deal was signed in January, will prevent the further collapse of bilateral relations between the two nations as U.S. Trade Representative Robert Lighthizer continues to engage with his Chinese counterparts.

At stake in this back-and-forth are billions of dollars in trade. In 2018, the U.S. imported \$539 billion worth of goods from China, and exported \$120 billion, including \$13 billion worth of agricultural and related products.¹ In 2019, while trade of goods between the two nations declined overall to \$452 billion in imports and \$106 billion in exports, U.S. agricultural exports increased to \$16 billion. The Phase One trade deal promised an additional \$200 billion in Chinese purchases of U.S. goods and services over the next two years. Included in the \$200 billion, were an additional \$32 billion in agricultural goods over the 2017 baseline of \$24 billion, for a total of \$36.5 billion in 2020 and \$43.5 billion in 2021, an extremely ambitious goal, which many analysts were skeptical of from the start.

China has indeed increased its purchases of U.S. products, particularly for manufactured goods, but as of June, it was only on pace to meet 47% of its targeted purchases and only 24% of its agricultural commitments. In other words, China has purchased only about \$8.7 billion worth of agricultural goods in the first half of 2020 and would need to import nearly \$28 billion worth of ag products between now and December 31 to meet the target, a prospect that seems increasingly unlikely.²



¹ Includes agricultural goods, as well as ethanol, biodiesel, forest products, and fishery products.

² Peterson Institute for International Economics, US-China Phase One Tracker.

Continued on next page

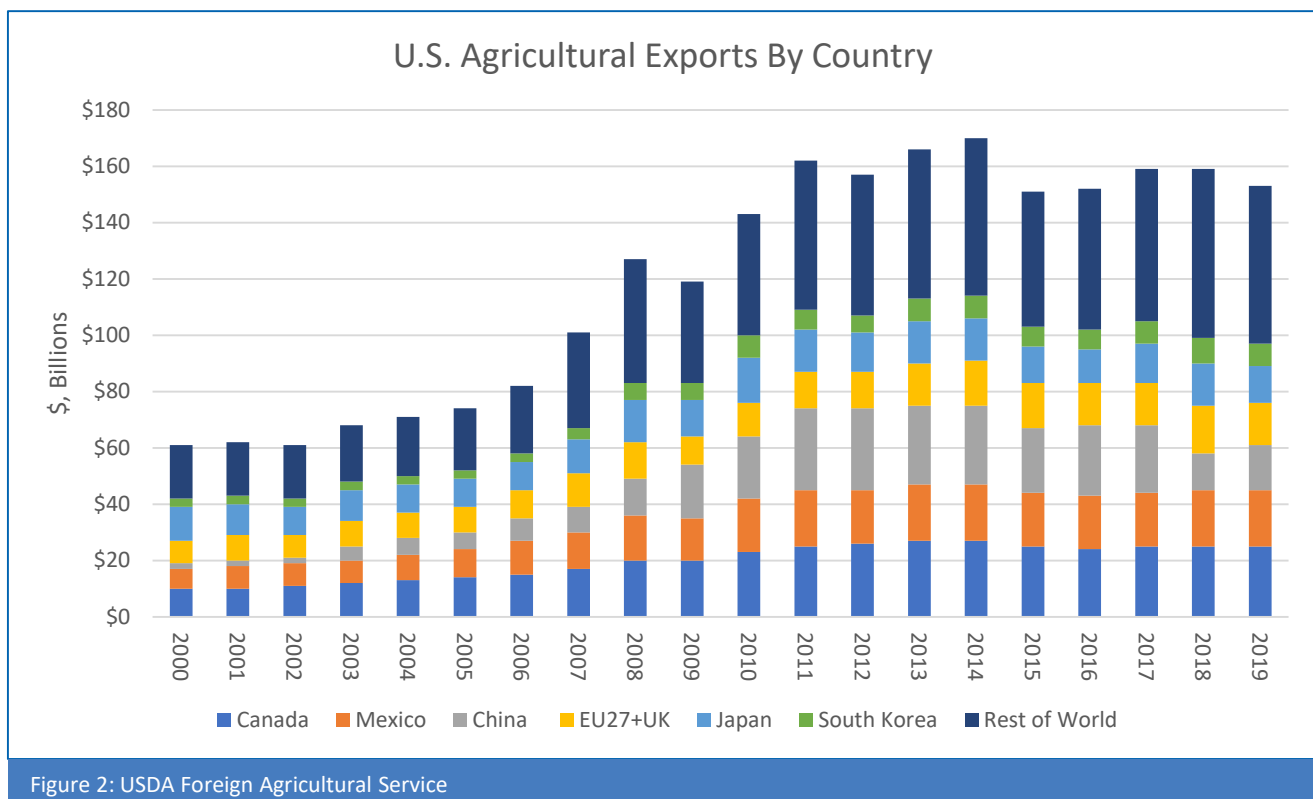
China is not the only source of trade concerns for U.S. agriculture. The U.S. and the European Union (EU) have a long-simmering trade dispute over subsidies to aerospace manufacturers Airbus and Boeing. While the origin of the dispute may be narrow, the fallout has been felt across a range of industries. The U.S. has imposed tariffs on approximately \$7.5 billion of European imports while the EU retaliated in a similar fashion.

In addition to tariffs on aircraft, the U.S. has imposed tariffs ranging from 15-25% on European dairy products, fruits, seafood, pork, olives, spirits, clothing and some manufactured goods. The EU has responded similarly, targeting many agricultural products.

Another trade issue the U.S. has long complained about is Europe's attempt to prohibit the use of "geographical indicators" by non-European products around the world. These include the use of names for a variety of wines, spirits and foodstuffs linked to a specific region, such as requiring the term Bourdeaux be applied only to wine produced in the Bourdeaux region of France, or that Parmigiano cheese must come from the Parma region of Italy.

Finally, the U.S. has taken issue with a number of non-tariff barriers to trade with Europe, such as limitations on the import of genetically modified agricultural products.

Recently, however, a sign of a potential thaw in relations has emerged as the European Commission agreed to end tariffs on U.S. lobster,³ a welcome development for an industry hit hard by trade disputes and the pandemic. In return, the U.S. will reduce its tariffs on a number of European goods. Both sides hope that this agreement will open the door to further normalization of trade relations.



³ BBC News, "US Wins End of EU Lobster Tariffs in Mini Trade Deal," August 21, 2020.

2019 U.S. Agricultural Exports By Category

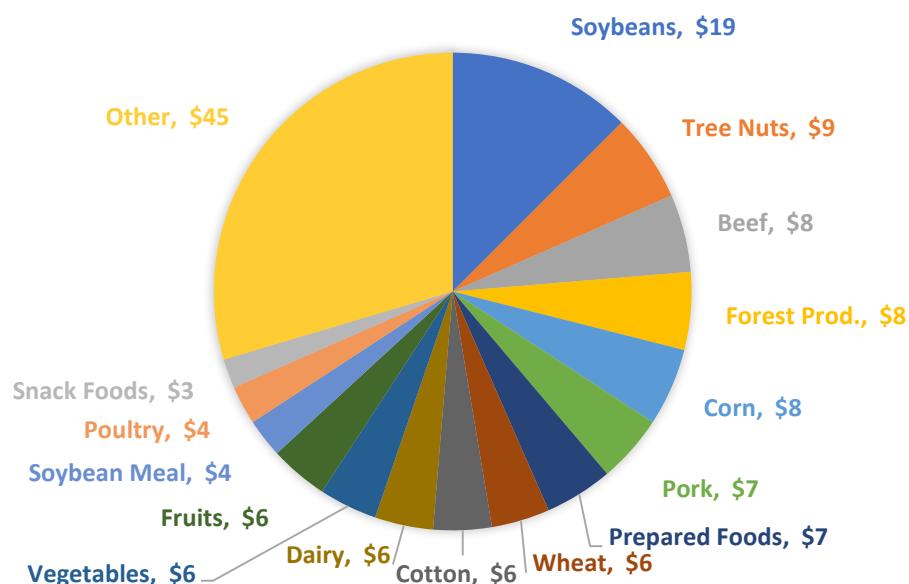


Figure 3: USDA Foreign Agricultural Service. Dollar Amounts in Billions.

Finally, there is trade between the U.S., Canada and Mexico. Many businesses reliant on North American trade breathed a sigh of relief when the USMCA was ratified earlier this year. While the changes in the USMCA were fairly modest compared to its predecessor, NAFTA, the potential lapse of an agreement was cause for concern. When NAFTA took effect in 1992, trade between the U.S., Canada and Mexico was approximately \$300 million annually. Today, it exceeds \$1 trillion as supply chains have become increasingly integrated between the three nations. Thus, the implementation of the USMCA was more about avoiding disruption in trade than increasing it.

Still, the agreement promises new export opportunities for some U.S. industries, including the dairy sector. When the agreement was signed, the International Trade Commission projected that U.S. dairy exports could increase by more than \$314 million per year. Much of this was based on increased access to the protected Canadian dairy market, a provision in the agreement that was controversial in that nation. Now that the USMCA has been implemented, some in the U.S. Congress are arguing that Canada is not fully complying with the agreement, by continuing to favor domestic producers and processors over those from the U.S.

In summary, international market access is essential for U.S. agriculture, and has become significantly more important since 2000. American farmers are among the most productive and efficient in the world and, increasingly, are producing far more than our domestic population consumes. Thus, access to the 96% of the world's population that lives outside our borders is critical. Even for producers whose products are not directly exported, domestic supply and demand, and market prices are significantly influenced by export markets.

There are certainly a number of legitimate issues for U.S. trade negotiators to raise with our partners around the globe. Addressing these issues, including tariffs and non-tariff barriers, protection of intellectual property, trademark enforcement and more, with as minimal fallout as possible makes the job of U.S. trade negotiators difficult, but essential, for U.S. agriculture.

CONTACT INFORMATION

We look forward to your questions about Knowledge Exchange Partner and your feedback:

KnowledgeExchange@FarmCreditEast.com

**KNOWLEDGE
EXCHANGE
PARTNER**

Farm Credit East Disclaimer: The information provided in this communication/newsletter is not intended to be investment, tax, or legal advice and should not be relied upon by recipients for such purposes. Farm Credit East does not make any representation or warranty regarding the content, and disclaims any responsibility for the information, materials, third-party opinions, and data included in this report. In no event will Farm Credit East be liable for any decision made or actions taken by any person or persons relying on the information contained in this report.



FARM CREDIT EAST