Securing the Credit Department and Avoiding Coronavirus-Related Fraud While Working from Home

Fraudsters will exploit just about anything if it means walking away with some financial or other confidential information—and that includes putting the COVID-19 pandemic to criminal use. Once the first U.S. case was reported in mid-January, many capable businesses, including their credit professionals, began operating remotely to comply with the nation's social distancing efforts. Unlike many workplaces and their top-of-the-line technical security features, home offices aren't necessarily as equipped, therefore, increasing the risk of a potential breach. In addition to utilizing previous anti-fraud measures, credit managers should be wary of coronavirus-related fraud to further protect company information from unwanted exposure.

The Federal Trade Commission (FTC) has identified several coronavirus-related scams currently roaming the business-to-business credit industry, some of which are already familiar to credit professionals, albeit with slight twists. First and foremost is the business email compromise scam (BEC) when a fraudster communicates with a company via email and impersonates the company's CEO or another higher-up to get confidential information. FTC states criminals are leaning on this tactic because companies are engaging in "a flurry of unusual financial transactions" during COVID-19, including expedited orders, cancelled deals, refunds, etc.

"That's why an emergency request that would have raised eyebrows in the past might not set off the same alarms now," FTC reported. "Compounding the problem is that teleworking employees can't walk down the hall to investigate a questionable directive."

Working remotely also makes companies more prone to tech scams. Similar to BEC fraud, IT scams are occurring with criminals impersonating an employee from a company's technology support staff and then offering to fix a tech issue or sharing a new link for software. To fix the "issue," FTC states, the fraudster requires access to the individual's computer and, if granted, could lead to financial and/or confidential exposure. Clicking on fraudulent links could also lead to similar losses.

With credit professionals now working from home, businesses either already have plans in place for secure remote working or are attempting to establish external security features. The former applies to Credit Manager Margaret Thompson, who said her company, Samuel, Son & Co., implemented a couple of steps within the past year due to a few instances of outside hackers attempting to access their data. Thompson said they have dual Microsoft verification that requires them to send a code to their cell phones when they need to enter the systems from outside the office on non-office equipment. Employees also have tokens provided by the company that sends a passcode allowing them to access and enter their network from home through a separate VPN connection.

"Even with this, perpetrators have attempted to access [our information], as I have received Microsoft verification attempts at the strangest times of day, including on the weekends and in the early morning hours," she said. "Our IT department traced these back to foreign countries

on the other side of the world. I have been told these attempts are made to anyone who does business in the money world."

Per the Payment Card Industry Data Security Standard (PCI DSS), Samuel, Son & Co. created a credit card form that customers must complete. Customers can only confirm the last four digits of their credit card number as well as the security code and expiration date, Thompson noted. Then, the company's system will store the credit card and expiration date but not the CVV code. If the company does not have the card on the customer's profile, they will personally contact the customer to obtain the complete credit card information from them. The customer information is completed over the phone when appropriate and the necessary documents are shredded if the customer has sent it via email. Credit card information on the customer's profile is only kept if the customer gives the company permission.

"I do not think we have seen any evidence of fraud in the credit arena during this pandemic," Thompson said. "I would just tell others to be smart—do not take unnecessary risks and if it something seems shady, it probably is."

After more than a month of working from home, MPW Industrial Services Credit and Collections Manager Lee Tompkins, RGCP, said all of his direct reports and those of all employees working from home connect to the company's servers through a VPN. Prior to everyone working remotely, all employees had to take two online courses a training team put together months ago from the company's Learning Management System. Those two courses covered working remotely and how to be safe with the internet as well as phishing scams and what emails should and should not be opened.

"I'm of the opinion we are just as safe working from home as we are working in the office," Tompkins said. "We still have some vulnerability at the office and that would apply to home as well. Those attacks mainly come via emails that contain links that could compromise our servers."

—Andrew Michaels, editorial associate