AiA Art News-service

INTERNATIONAL EDITION
THE ART NEWSPAPER

Galleries hit by cyber crime wave

Hackers are using an email scam to intercept payments between galleries, collectors and others

CRISTINA RUIZ, ANNA BRADY, SARAH P. HANSON and JULIA MICHALSKA
31st October 2017 08:21 GMT

Galleries are being targeted by cyber criminals Blake Connally

Hackers are stealing large sums of money from art galleries and their clients using a straightforward email deception. The Art Newspaper has so far identified nine galleries or individuals targeted by this scam. They include Hauser & Wirth, the London-based dealers Simon Lee, Thomas Dane, Rosenfeld Porcini and Laura Bartlett and, in the US, Tony Karman, the president of Expo Chicago.

“We know a number of galleries that have been affected. The sums lost by them or their clients range from £10,000 to £1m,” says the insurance broker Adam Prideaux of Hallett Independent. “I suspect the problem is a lot worse than we imagine.”

How it works

The fraud is relatively simple. Criminals hack into an art dealer’s email account and monitor incoming and outgoing correspondence. When the gallery sends a PDF invoice to a client via email following a sale, the conversation is hijacked. Posing as the gallery, hackers send a duplicate, fraudulent invoice from the same gallery email address, with an accompanying message instructing the client to disregard the first invoice and instead wire payment to the account listed in the fraudulent document.

Once money has been transferred to the criminals’ account, the hackers move the money to avoid detection and then disappear. The same technique is used to intercept payments made by galleries to their artists and others. Because the hackers gain access to the gallery’s email contacts, the scam can spread quickly, with fraudulent emails appearing to come from known sources.

The victims

This summer, the London-based dealer Laura Bartlett sold a group of works to a US collector. “It was quite a high-value sale for me,” she says. The transaction was negotiated entirely by email and when it was finalised, Bartlett sent the buyer an invoice via email, as she has sent all her invoices for the past 12 years. Her client received this but soon afterwards, Bartlett’s emails were intercepted. “Somebody sent out another email saying: ‘Ignore my previous

invoice. I sent you old bank details; please use this invoice instead.'" The client duly wired the money to the hackers instead of to Bartlett.

"I kept checking my account to see if the money had arrived and sending more and more emails to my client to ask where the funds were," she says. Her client responded to these emails, but "in retrospect, I realise that the tone of his emails had completely changed", Bartlett says. What she and her client did not know at the time was that the hackers were now controlling all correspondence between them while impersonating them both. The hackers responded to Bartlett's queries about the payment with reassurances that "everything was fine and that the delay in receiving payment was being looked into".

It was only when Bartlett called the client a week later that they both realised what had happened. They reported the theft to the Action Fraud team at the Metropolitan Police in London but have no information about the ongoing investigation. (A spokesman for Action Fraud told The Art Newspaper that Bartlett and her client's "reports have been reviewed and have been disseminated to the Metropolitan Police service for investigation".)

Bartlett's client has not recovered his money and is unlikely to do so. "His bank told him that it was not able to recompense him," Bartlett says. In cases such as these, "the bank has not made an error for which it necessarily has to take responsibility", says Chris Bentley, the director of underwriting at AXA Art Northern Europe, Middle East and Asia Pacific.

Some art dealers believe that banks should carry out more detailed checks on new clients before they are allowed to open accounts. Ian Rosenfeld of Rosenfeld Porcini in London has been trying to recover money stolen from one of his gallery's clients for 18 months. As in Bartlett's case, the theft occurred after criminals intercepted an email invoice sent to a client following the sale of a work.

"Around seven or eight hours after we had sent our invoice, the buyers got another email saying that the invoice we had sent out

was in the wrong currency and that they should make payment to a different account," Rosenfeld explains. Once again, the collectors wired the funds to an account set up by fraudsters. "We're still in discussion with the bank a year and a half later, trying to recover the money; they have been completely useless," Rosenfeld says.

The art world is not being specifically targeted by hackers, but the fast-paced transactions and large sums of money changing hands make it particularly lucrative. "You can't buy a $1m condo without three weeks of paperwork and 100 checks and balances, but art dealers and their clients will wire $1m after a single conversation," says one US dealer who asked not to be named. The same dealer, whose gallery nearly lost $500,000 when one of his clients wired money to a fraudster (the client was able to recover the funds after the bank questioned the transfer), says he knows of many more galleries targeted by hackers.

For Bartlett, the loss of income from a major sale came at a bad time. "I didn't have the financial security to weather this kind of scenario," she says. "If it had happened at another time of year, when I'd had a better run, it might have been OK, but this particular sale was going to pay a lot of bills." Shortly after the cyberattack, Bartlett closed her gallery.

Other London-based dealers who have lost money through this type of fraud include Simon Lee. "Our accountant received an email and invoice from someone within our company, with a message saying 'please pay this'," he says. The sum lost by Lee's gallery was small, he says, but he knows "people who have been taken for hundreds of thousands of pounds". Lee now issues a standard warning about cyberfraud with every invoice and his accountant now "telephones and confirms banking instructions with clients over the phone".

In the US, a similar fraud attempt targeted Expo Chicago. "Someone got into our system," says president Tony Karman. "We have a good system, but someone got in and sent an email to our accountant from my email address with an invoice and a message that said 'please pay this immediately'. Fortunately, our accountant

checked the invoice with me and I told him ‘I didn’t send it; it wasn’t me. We immediately put extra security measures in place.”

Back in London, another victim is Thomas Dane; the gallery lost money when it inadvertently wired money to a fraudster’s account. “It was a staggered payment that got intercepted,” says François Chantala, a partner at the gallery. “It has been a wake-up call to completely overhaul our invoicing procedures,” he says, adding that the gallery now sends most of its invoices by courier.

It is not just small or mid-size galleries that have been targeted. The Swiss gallery Hauser & Wirth, which has spaces in London, Somerset, Zurich, New York and Los Angeles, has also been a victim of the scam. In response to our questions, the gallery said in a statement: “Like many others, it’s true that we were targeted by a cyberattack. Due to the systems we have in place and the vigilance of our team, as soon as the fraud attempt occurred we responded swiftly, resulting in a full recovery of the funds. We are very aware of the potential risks that digital transactions bring and have implemented additional security measures to protect our staff and contacts.”

Raising awareness

Art dealers’ associations have been trying to raise awareness of cyber-security for months. In February, the Society of London Art Dealers issued a warning to its members about the dangers of email fraud. Three months later, it sent out the warning again. In the US, the Art Dealers Association of America (ADAA) circulated its first warning on cyber-risks, including this specific type of email fraud, which it refers to as a “man-in-the-middle” scam, in 2016. Adam Sheffer of the gallery Cheim & Read, who is the president of the ADAA, says that he issued the alert after being approached by “high-profile American and European galleries”, as well as artists who had been targeted by scammers.

Taking basic precautions such as encrypting invoices and confirming bank details over the phone with clients, artists and service providers before money is transferred is critical, not least because insuring against loss from an email fraud or other hacks is

difficult. Although some cyber-insurance policies do exist, these typically have a relatively low cap on the losses that can be claimed. Furthermore, if these policies are bought by galleries, they will only protect the galleries themselves, and not their clients, who are often the victims.

The insurance industry is divided about the efficacy of such products. AXA Art does not currently offer a policy that will protect against loss from this type of email fraud, Bentley says. “This is a very rapidly evolving area for the insurance market,” he says. “It’s moving so quickly that if you renewed your policy in April rather than October, you might have a different arrangement.” He believes that it is more effective for galleries to adopt “a change in practice to avoid this situation happening in the first place rather than buying what is going to be potentially quite expensive insurance. Even if an insurance solution is eventually offered, it is still likely to be both limited and expensive.”

For galleries in the UK, introducing greater security is critical. Next May, the UK will implement new EU legislation: the General Data Protection Regulations. (The legislation will be introduced in Britain regardless of Brexit.) These require every company that stores personal data, such as clients’ email addresses, to protect it adequately. So, if your gallery’s email account is hacked because of inadequate security measures, you could be fined 4% of your annual turnover or €20m, whichever is higher. “No galleries are that aware of the impending regulation,” Lee says, adding that, for galleries, “there are huge responsibilities involved and there is a lot to do in preparation”.

Five-step protection against email fraud

1 Regularly change all passwords for email, software and wifi

2 Ensure all anti-virus software is up to date

3 Only send invoices by email if they have been encrypted (password-protected)

4 After sending or receiving an invoice by email, call and/or send a text or WhatsApp message to the recipient to double-check the sort code and account number

5 Urge all staff to be extremely vigilant when opening emails and do not download any attachments or click on web links from an untrusted source. Always confirm legitimacy over the telephone with the sender if in doubt

• To contact us about cyber crime, please email londonoffice@theartnewspaper.com